Product Guide

McAfee Endpoint Protection for Mac 2.1.0

COPYRIGHT

TRADEMARK ATTRIBUTIONS

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement

Contents

Preface 7

About this guide . . . 7

Audience . . . 7

Conventions . . . 7

Find product documentation . . . 8

1 Introduction 9

Why you need security for Mac . . . 9

How McAfee Endpoint Protection for Mac protects your system . . . 10

Anti-malware . . . 10

Desktop firewall . . . 10

Application protection . . . 11

Product features . . . 11

2 Installation and deployment 15

System requirements . . . 15

Package contents . . . 16

Install the software on a standalone Mac . . . 16

Install the software using wizard . . . 16

Install the software from the command line (silent installation) . . . 16

Upgrade the software . . . 17

Upgrade the software on a standalone Mac . . . 17

Upgrade the software on a managed Mac . . . 17

Default settings . . . 19

Recommended post-installation tasks . . . 20

Deploy the software on a managed Mac . . . 21

Check in the package using software manager . . . 21

Install the extensions using software manager . . . 22

Check in the package manually . . . 22

Install the extensions manually . . . 23

Deploy McAfee Endpoint Protection for Mac from ePolicy Orchestrator . . . 23

Test the installation . . . 24

Test the anti-malware protection feature . . . 24

Test the application protection feature . . . 24

Test the desktop firewall feature . . . 25

Uninstall the software . . . 26

Uninstall the software from a standalone Mac . . . 26

Remove the software from a managed Mac . . . 27

3 Using the software on a standalone Mac 29

Dashboard . . . 29

Security status . . . 29

Recent events summary . . . 30

History of events . . . 30

Quarantine malware . . . 31

Remove or restore the quarantined item . . . 31
Update the anti-malware and DAT files . . . 31
Perform a system scan . . . 32
Configure custom scan tasks . . . 32
Create a scan task . . . 32
Modify an existing scan task . . . 33
Remove an existing scan schedule . . . 33

4 Configuring protection preferences on a standalone Mac 35

General preferences . . . 35
Configure general preferences . . . 35
Anti-malware . . . 36
Configure on-access scan preferences . . . 36
Configure on-demand scan preferences . . . 37
Define anti-malware exclusions . . . 38
Best practices for anti-malware preferences . . . 38
Application protection . . . 39
Configure preferences for application protection . . . 39
Create an application protection rule . . . 40
Modify an existing application protection rule . . . 41
Reapply rules for modified applications . . . 41
Specify exclusions for application protection . . . 41
Best practices for application protection . . . 42
Desktop firewall . . . 43
How stateful filtering works . . . 44
How regular mode firewall protection works . . . 44
How Adaptive mode firewall protection works . . . 45
How DNS blocking works . . . 46
How stateful FTP inspection works . . . 46
How desktop firewall rules work . . . 47
How desktop firewall rules are organized . . . 48
Create a firewall rule . . . 49
Desktop firewall rules examples . . . 51
Best practices for desktop firewall . . . 53
Configure an update schedule . . . 54
Configure the repository list . . . 54
Configure proxy settings . . . 54
Configure the anti-malware update schedule . . . 55

5 Managing the software with ePolicy Orchestrator 57

Manage policies . . . 57
Create or modify policies . . . 58
Assign policies . . . 58
Create a self-protection policy . . . 59
Create an anti-malware policy . . . 59
Schedule an anti-malware update . . . 61
Schedule an on-demand scan . . . 62
Create an application protection policy . . . 63
Desktop firewall policy . . . 64
Create a desktop firewall policy . . . 64
Create firewall rules . . . 65
Create a rule group and move rules to the group . . . 66
Create a DNS blocking policy . . . 67
Create a trusted networks policy . . . 67
Create a location awareness policy . . . 68
Queries and reports . . . 69

Run a query 69

6 Troubleshooting 71

Run the repairMSC utility 71

Index 73

Preface

This guide provides the information you need for all phases of product use, from installation to configuration to troubleshooting.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
ℹ	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
❗	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1. Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.
2. Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

McAfee® Endpoint Protection for Mac offers scalable security solution that minimizes the risk of exposing your Mac to vulnerabilities.

The software provides a securely configured environment that:

- Protects your Mac from viruses, spyware, trojan horses, and other malware threats.
- Prevents unauthorized network access.
- Prevents execution of unwanted application.
- Restricts applications to run with restricted or without network access.

Contents

- *Why you need security for Mac*
- *How McAfee Endpoint Protection for Mac protects your system*
- *Product features*

Why you need security for Mac

Systems without protection may result security breach in many ways such as data loss, misuse of personal and business information, and system disorder.

New products and technologies broaden opportunities for new security threats and challenges. The motive behind these threats is to interrupt and espionage your system or destruct the data and the system functionality completely.

The targeted security threats devised by cyber criminals and hackers are evolving consistently and increasing the risk consistently. The analyst reports say that the overall malware samples reached more than a 100 million implying the importance of securing your Mac from the threats.

The list of threats and reported vulnerabilities that can harm your Mac are:

Threat category	Potential threat
Malware	Directs the user to access malicious items that can infect a Mac. Examples: Flashback Trojan, Fake AV
Spyware	Tracks every key you type to access sensitive information, such as user name and password and other personal details. Example: Keyloggers

Threat category	Potential threat
Botnet breakdowns	Infects your system or network and controls it from remotely to spread malware.
Network threat	Slows down network performance and gain unauthorized access to systems.

With McAfee Endpoint Protection for Mac is enabled, your Mac is protected from these malware threats without compromising the needs. The software also provides a secured environment that eliminates the risk to exposing to these vulnerabilities.

How McAfee Endpoint Protection for Mac protects your system

McAfee Endpoint Protection for Mac provides a comprehensive security mechanism that includes anti-malware, desktop firewall, and application protection.

Anti-malware

Anti-malware protection secures your Mac from malware threats proactively with the predefined actions upon detecting malware and suspicious items.

When enabled, the anti-malware feature scans files, folders on local, network-mounted volumes, and removable media whenever you create or access an item.

The anti-malware engine:

- Performs complex analysis using the malware definition files (DATs)
- Decodes the contents of the item you access
- Compares them with the known signatures stored in the DAT files to identify malware

For more information, see *Anti-malware preferences*.

Desktop firewall

Filters incoming and outgoing network traffic, to allow or block them as defined in the rules. Each rule defines a set of conditions that the network traffic must meet and the rule's associated action is executed.

Stateful filtering and packet inspection identify data packets for different types of connections and hold the connection attributes in memory until the end of the session. When the first data packet of a new session arrives, desktop firewall matches the packet against the rules list. If the data packet matches an existing allow rule, a new entry is added to the state table and the traffic is allowed, and its subsequent packets are allowed without further verification for that session. When the session is completed or timed out, the entry is removed from the table.

If the data packet does not match existing rules, firewall blocks the network traffic.

You can run the desktop firewall protection in:

- **Regular mode** — When the network packet adheres to a rule’s condition, the associated action defined in the rule is executed. If no matching rule is found, the network packet is blocked.
- **Adaptive mode** — When the network packet matches a rule’s conditions, the associated action defined in the rule is executed. If no matching rule is found, the packet is allowed and a rule is created to allow similar packets later.

Controlled network access protection permits the Mac to access only authorized networks, minimizing the risk from network threats.

For more information, see *Configuring protection preferences*.

Application protection

Configure rules to prevent execution of applications or to run applications with restricted or without network access.

You can set rules for the applications installed on a Mac to:

- Execute with full network access
- Execute without network access
- Execute with restricted network access
- Block the application execution

For example, you can configure iTunes to use for recreational purposes only, so that it can't access the Internet for downloading music. You do this by selecting **allow execution without network access**.

For more information, see *Configure preferences for application protection*.

Product features

The main features of McAfee Endpoint Protection for Mac are described in this section.

Anti-malware

- **Anti-spyware protection** — Protects the Mac from spyware threats.
- **On-access Scan** — Scan files and folders whenever users access them.
- **Performance improvements for On-demand-Scan (ODS)** — Completes scan files and folders faster with less resource.
- **Quarantine** — Quarantine malware items (or suspected malware-like behavior) so that they can't be opened or executed.
- **Schedule Scan** — Define schedules to scan files and folders on local and mounted volumes.
- Separate regular expression based exclusion for on-access scan and on-demand scan.
- Scan network volume, compressed files, and emails.

Desktop firewall

- **Regular mode** — When the network packet adheres to a rule’s condition, the associated action defined in the rule is executed. If no matching rule is found, the network packet is blocked.
- **Adaptive mode** — When the network packet matches a rule’s conditions, the associated action defined in the rule is executed. If no matching rule is found, the network packet is allowed and a rule is created to allow similar packets later.
- **Stateful firewall** — The stateful filtering and network packet inspection validate each packet for different connections against predefined rules, holding the connection attributes in memory from beginning-to-end.
- **Domain Name System (DNS) block** — Blocks access to unwanted domains.
- **Stateful FTP inspection** — Desktop firewall automatically creates dynamic rules for FTP data connections, by actively monitoring the FTP commands on the control channel.
- **Trusted networks** — You can define networks that can include subnets, ranges, or a single IP address that can be used while creating firewall rules.
- **Location awareness** — Creates separate rules for locations, such as office or home network.
- **Common ePolicy Orchestrator extension for managing Host IPS Firewall on Windows and Mac** — When your Mac is managed by ePolicy Orchestrator, a common extension (Host IPS Firewall) is used for Windows and Mac.

Application protection

- **Block application execution** — Prevent execution of applications installed on your Mac.
- **Restricted or full network access for applications** — Configure applications to run with full or restricted network access.
- **Run applications without network access** — Configure applications to run without network access.

Interface

- **McAfee menulet for easy access** — Access the McAfee menulet 🛡 to launch the McAfee Endpoint Protection for Mac **Console**, McAfee Endpoint Protection for Mac **Preferences**, and the **About McAfee Endpoint Protection for Mac** dialog box.
  - **Dashboard** — View the security status of your Mac, scheduled scan tasks, latest events, and the anti-malware update details.
  - **History of events** — View all anti-malware and application protection events.
  - **Enhanced client user interface** — Allows you to define preferences.
  - **Notifications** — **McAfee Notification** displays:
    - Detection of malware (resulting from on-access scan)
    - Prevention of application execution
    - Denial of network access to applications
  - **Alerts** — Get **McAfee Alert** for an unknown or modified application execution when you set the corresponding application protection setting as **Prompt**.

General

- **Self protection** — Allows ePolicy Orchestrator administrators to enable password protection in the client interface to prevent local users from modifying the defined policy preferences, and to uninstall the software on managed Macs.

2 Installation and deployment

Install McAfee Endpoint Protection for Mac on a standalone (unmanaged) Mac, or deploy from ePolicy Orchestrator on a managed Mac.

> ! When you install McAfee Endpoint Protection for Mac on Mac OS X server, only the Anti-malware component is installed. The Application Protection and Desktop Firewall components are not installed.

Contents

- *System requirements*
- *Package contents*
- *Install the software on a standalone Mac*
- *Upgrade the software*
- *Default settings*
- *Recommended post-installation tasks*
- *Deploy the software on a managed Mac*
- *Test the installation*
- *Uninstall the software*

System requirements

Make sure that your Mac meets these requirements and that you have administrator rights.

Component	Requirement
Operating system	• Lion 10.7.x and later • Mountain Lion 10.8.x and later • Mavericks 10.9 and above • Mac OS X server
Hardware	Mac that can run with the supported operating system configuration.
McAfee management software	McAfee ePolicy Orchestrator 4.6.x and 5.0.x.
McAfee Agent (required for ePolicy Orchestrator deployment)	McAfee Agent for Mac 4.8 Patch 1 and later.
McAfee Host Intrusion Prevention	8.0.3.762 and later

Package contents

The software package contains these files that are necessary for installation.

Package	Description
EPM<version>-<release-type>-<build-number>.dmg	Contains files to install the software on standalone Mac.
EPM<version>-<release-type>-ePO-<build_number>.zip	Contains files to deploy the software from the ePolicy Orchestrator server.

Install the software on a standalone Mac

Install the software on a standalone Mac using the wizard or from the command line.

Tasks

- *Install the software using wizard* on page 16
  The wizard guides you through the steps to install the software on your Mac.
- *Install the software from the command line (silent installation)* on page 16
  You can use the command line to install the software without user intervention.

Install the software using wizard

The wizard guides you through the steps to install the software on your Mac.

> ! When the installation is complete, McAfee Endpoint Protection for Mac starts protecting your system immediately. Any existing network connections on your Mac are disconnected. You must re-establish those connections.

Task

1. Download EPM<version>-<release-type>-<build-number>.dmg to a temporary location on your Mac, then double-click it to mount EPM<version>-<release-type>-<build-number>.pkg.
2. Double-click EPM<version>-<release-type>-<build-number>.pkg to open the wizard.
3. Follow the prompts to install the software.

Install the software from the command line (silent installation)

You can use the command line to install the software without user intervention.

> ! When the installation is complete, the software starts protecting your Mac immediately. Any existing network connections that are running on your Mac are disconnected. You must re-establish those connections.

Task

1. Download EPM<version>-<release-type>-<build-number>.dmg, then double-click it to mount EPM<version>-<release-type>-<build-number>.pkg file.
2. Copy the EPM<version>-<release-type>-<build-number>.pkg file to a temporary location on your Mac.
3. Open a Terminal window and change the working directory to the one where you saved the EPM<version>-<release-type>-<build-number>.pkg file.

4 Type the following command, then press **return**.

```
sudo installer -pkg EPM<version>-<release-type>-<build-number> .pkg -target /
```

5 Type the administrator password, then press **return**. The following message appears.

```
The Install was successful.
```

Upgrade the software

McAfee Endpoint Protection for Mac supports upgrading the software and migrating the configuration from the previous versions of the software.

Upgrade the software on a standalone Mac

You can upgrade the software and migrate the existing configuration settings.

You can upgrade the software from:

- McAfee Security for Mac 1.1 and later to McAfee Endpoint Protection for Mac 2.1

  > When the software is upgraded, only the Anti-malware and Application Protection preferences and rules are migrated. The Desktop Firewall rules are not migrated during the upgrade.

- McAfee Endpoint Protection for Mac 2.0 to McAfee Endpoint Protection for Mac 2.1

  > When the software is upgraded, the Anti-malware, Application Protection and Desktop Firewall preferences and rules are migrated during the upgrade.

- McAfee VirusScan for Mac 9.1 and later to McAfee Endpoint Protection for Mac 2.1

Before upgrading the software, make sure that these system requirements are met:

- Operating system
- ePolicy Orchestrator
- McAfee Agent

  > If the minimum required version of McAfee Agent is not found in the Mac during the upgrade, the installation program upgrades McAfee Agent also.

When a previous version of the software is found during the installation, the installation program upgrades the software to the new version. To upgrade the software:

1 Install the software using the wizard.

  For more information, see *Install the software using wizard*.

2 Make sure that all existing rules and preferences are migrated to the new version.

Upgrade the software on a managed Mac

When you upgrade the extension, the existing policies are migrated and the existing reports are upgraded to the new version.

You can upgrade the software from:

- McAfee Security for Mac 1.1 and later to McAfee Endpoint Protection for Mac 2.1

  > When the software is upgraded, only the Anti-malware and Application Protection policies are migrated and these policies will co-exist with the new policies. The Desktop Firewall policies are not migrated.

- McAfee Endpoint Protection for Mac 2.0 to McAfee Endpoint Protection for Mac 2.1

  > When the software is upgraded, existing Anti-malware, Application Protection and Desktop policies are migrated and these policies will co-exist with the new policies.

- McAfee VirusScan for Mac 9.1 and later to McAfee Endpoint Protection for Mac 2.1

Before upgrading the software, make sure that the system requirements are met:

- Operating system
- ePolicy Orchestrator
- McAfee Agent

  > If the minimum required version of McAfee Agent is not found in the managed Mac, the upgrade will fail.

- McAfee Host Intrusion Prevention extension 8.0.3.762 and later.

  > For more information, see *System Requirements*.

Make sure that you take a backup of existing policies for the existing version of the product. For instructions about backing up policies, see the ePolicy Orchestrator product guide of your version.

When the Anti-malware only extension is migrated, the anti-spyware default settings are applied.

ePolicy Orchestrator reports extensions are upgraded and events from the earlier version can be used for queries. After migration, all the queries from the earlier version are available under the new version.

1. Check in and deploy the extension.

   For more information, see *check in the package* and *install the extensions*.

2. Make sure that the policies are migrated properly and the reports are upgraded to the new version.
3. Deploy the product.

Default settings

Once installed, McAfee Endpoint Protection for Mac starts protecting the Mac immediately based on the default configurations defined. Refer to these default settings, and configure them for your environment.

Anti-malware

Feature	Default settings
General	**On-access Scan** — On **Spyware Scan** — On **Application Protection** — On **Desktop Firewall** — On
Anti-malware	**On-access Scan**: • **Scan files while** — Write • **Maximum scan time for a file** — 45 seconds for a file. • **When a virus is found** — Clean • **If clean fails** — Quarantine • **When a spyware is found** — Clean • **If clean fails** — Quarantine **Also scan**: • **Archives & Compressed Files** — Disabled • **Apple Mail messages** — Disabled • **Network Volumes** — Disabled
	On-demand Scan: • **When a virus is found** — Clean • **If clean fails** — Quarantine • **When a spyware is found** — Clean • **If clean fails** — Quarantine • **Archives & Compressed Files** — Enabled • **Apple Mail messages** — Enabled • **Network Volumes** — Enabled
	Exclusions — None.
Update	In **Repository List** • **Repository Name** — McAfeeHttp, McAfeeFtp In **Proxy Settings** • **Proxy settings** — Do not use a proxy In **Schedule** • **Schedule** — Daily at 4:45 PM (local time)

Desktop Firewall

Feature	Default settings
Desktop firewall	• **Regular Mode** — Enabled • **Trust Local Subnet** — Selected For default firewall rules, see *Desktop firewall*.

Application Protection

Feature	Default settings
Application Protection	**Rules** • **Allow All Apple signed binaries** — Allowed • **Unknown/Modified Applications** — Allow **Exclusions** — None.

Recommended post-installation tasks

Perform these tasks to keep the anti-malware and DAT files up to date, and to make sure that the protection configuration does not affect the business routines.

Task	Description
Update anti-malware and DAT files	After installation, McAfee Endpoint Protection for Mac automatically updates the DAT files to protect the Mac from the latest threats. By default, this update is scheduled at 4.45 pm local time every day. When the DAT files are updated for the first time, it may take longer time to download the full DAT. The subsequent updates will be incremental. For more information, see *Update the anti-malware and DAT files*.
Perform an on-demand scan	Run an on-demand-scan to scan the local volumes, after you install the software to clean the infected files that are not accessed by but reside in the Mac.

Task	Description
Anti-malware protection	McAfee Endpoint Protection for Mac comes with the default settings for anti-malware protection. Verify that the default settings are consistent with your organization policies and provides complete protection against malware. Configure the **On-demand Scan** task to define: • The items to scan (files, folders, and drives) • Set frequency of scan (daily, weekly, monthly, or immediately) • Define the action when malware is found (**Delete** or **Quarantine**) ℹ For more information, see *Configure protection preferences*.
Desktop firewall	McAfee Endpoint Protection for Mac comes with the *stateful* desktop firewall enabled, which protects your Mac from the moment the product is installed. The firewall comes with a set of default rules that enable your Mac to access the necessary services. We recommend that you review the default rules to make sure that your Mac can access the necessary services according to your organization policies. The rules are processed using a top-down approach with the implicit default block rules that deny all traffic. This rule can't be modified. ℹ For more information, see *Desktop firewall*.

Deploy the software on a managed Mac

Deploy McAfee Endpoint Protection for Mac remotely to a client system in your network using ePolicy Orchestrator.

You can check in and install the packages and extensions in two ways:

- Check in the package and extension using Software Manager.
- Check in the package and extensions manually.

Tasks

- *Check in the package using software manager* on page 21
  You can check in, update, and remove McAfee Endpoint Protection for Mac using the Software Manager.
- *Install the extensions using software manager* on page 22
  You can install the extensions using the Software Manager.
- *Check in the package manually* on page 22
  Check in the McAfee Endpoint Protection for Mac deployment package to the ePolicy Orchestrator master repository.
- *Install the extensions manually* on page 23
  Install McAfee Endpoint Protection for Mac extensions using ePolicy Orchestrator.
- *Deploy McAfee Endpoint Protection for Mac from ePolicy Orchestrator* on page 23
  Use ePolicy Orchestrator to deploy the software to systems in your network that are managed.

Check in the package using software manager

You can check in, update, and remove McAfee Endpoint Protection for Mac using the Software Manager.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator as an administrator.
2. Click **Menu**, **Software**, then click **Software Manager**.
3. In the **Software Manager** page **Product Categories** list, select **Software (By Label)**, select **McAfee Endpoint Protection for Mac 2.1**, select EPM<version>-<release-type>-ePO-<build_number>, then click **Check in All**.

Install the extensions using software manager

You can install the extensions using the Software Manager.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator as an administrator.
2. Click **Menu**, **Software**, then click **Software Manager**.
3. In the **Software Manager** page **Product Categories** list, select **Software (By Label)**, select **McAfee Endpoint Protection for Mac 2.1**, select the following extensions, then click **Check in All**:
   - **Endpoint Protection for Mac 2.1.0:Anti-malware**
   - **Endpoint Protection for Mac 2.1.0:General**
   - **Endpoint Protection for Mac 2.1.0:Application Protection**
   - **Host Intrusion Prevention** (Desktop firewall features)
   - **Endpoint Protection for Mac 2.1.0:Anti-malware Reporter**
   - **Endpoint Protection for Mac 2.1.0:Application Protection Reporter**

Check in the package manually

Check in the McAfee Endpoint Protection for Mac deployment package to the ePolicy Orchestrator master repository.

Task

For option definitions, click **?** in the interface.

1. Download the EPM<version>-<release-type>-ePO-<build_number>.zip file to a temporary location on the ePolicy Orchestrator server.
2. Log on to the ePolicy Orchestrator server as an administrator.
3. Click **Menu** | **Software** | **Master Repository**, then click **Action** | **Check In Package**.
   a. For **Package type**, select **Product or Update (.ZIP)**.
   b. Click **Choose File**, select EPM<version>-<release-type>-ePO-<build_number>, click **Choose**, then click **Next**.
4. Select **Current**, then click **Save**.

Install the extensions manually

Install McAfee Endpoint Protection for Mac extensions using ePolicy Orchestrator.

You must install these extensions to enable the features of the product:

- **Endpoint Protection for Mac 2.1.0:Anti-malware**
- **Endpoint Protection for Mac 2.1.0:General**
- **Endpoint Protection for Mac 2.1.0:Application Protection**
- **Host Intrusion Prevention** (Desktop firewall features)
- **Endpoint Protection for Mac 2.1.0:Anti-malware Reporter**
- **Endpoint Protection for Mac 2.1.0:Application Protection Reporter**

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Software** | **Extensions**, then click **Install Extension**.
3. Click **Choose File** and select the file that contains the extension, then click **OK**.

Deploy McAfee Endpoint Protection for Mac from ePolicy Orchestrator

Use ePolicy Orchestrator to deploy the software to systems in your network that are managed.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. On the **Assigned Client Tasks** tab, click **Actions**, then click **New Client Task Assignment**.
4. Complete these options, then click **Create New Task**:
   a. For **Product**, select **McAfee Agent**.
   b. For **Task Type**, select **Product Deployment**.
5. On the **Client Task Catalog** page:
   a. Type a name for the task.
   b. Select **Mac** as the target platform.
   c. In **Products and components**, select **McAfee Endpoint Protection for Mac <version_number> <build_number>**, select **Install** as the action, then click **Save**.
6. In the **Client Task Assignment Builder** page:
   a. Select the task, then click **Next**.
   b. Schedule the task to run immediately, click **Next** to view a summary of the task, then click **Save**.
7. In the **System Tree**, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
8. Select **Force complete policy and task update**, then click **OK**.

Test the installation

When you have completed the installation, we recommend that you test it to make sure that the software is installed properly and can protect the Mac.

Tasks

- *Test the anti-malware protection feature* on page 24
  You can test the anti-malware protection feature by accessing the European Institute of Computer Anti-Virus Research (EICAR) standard anti-virus test file.
- *Test the application protection feature* on page 24
  You can test the application protection feature by creating a rule to deny application execution.
- *Test the desktop firewall feature* on page 25
  Test the desktop firewall feature by creating a rule. Consider a scenario where you want to create an allow rule for *www.abcwebsite.com*.

Test the anti-malware protection feature

You can test the anti-malware protection feature by accessing the European Institute of Computer Anti-Virus Research (EICAR) standard anti-virus test file.

This file is the combined effort by anti-virus vendors to implement one standard that customers can use to validate the anti-virus software.

Task

1. Go to the EICAR website http://www.eicar.org.
2. Click **DOWNLOAD ANTI MALWARE TESTFILE**, then click **DOWNLOAD**.
3. Click an anti-malware test file. For example, eicar.com.txt.

For the test to be successful, McAfee Endpoint Protection for Mac displays a message Notification `1 detection(s) found on your system` with the relevant details.

Test the application protection feature

You can test the application protection feature by creating a rule to deny application execution.

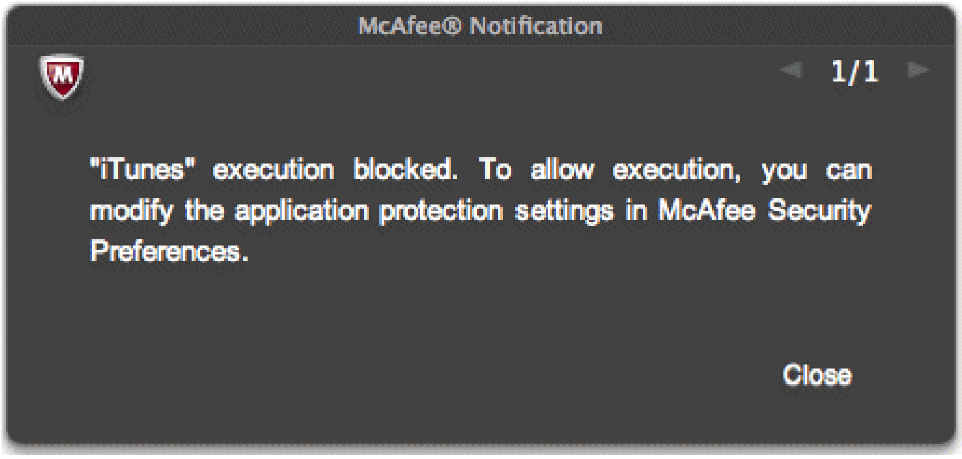
Consider a scenario where you want to block iTunes on your Mac.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. Click **Application Protection**.
3. Click 🔒, type the administrator password, then click **OK**.
   a. In **Rules**, click + in the bottom left corner of the console.
   b. In **Application Name**, browse and add **iTunes**.
   c. In **Action**, select **Deny Execution**, then click **OK**.

4 Click 🔓 to prevent further changes.

5 From the Dock, click **Finder**, **Go** | **Applications** | then double-click **iTunes** to display this message.



McAfee® Notification

1/1

"iTunes" execution blocked. To allow execution, you can modify the application protection settings in McAfee Security Preferences.

For more information on application preferences, see *Configuring protection preferences on a standalone Mac*.

Test the desktop firewall feature

Test the desktop firewall feature by creating a rule. Consider a scenario where you want to create an allow rule for *www.abcwebsite.com*.

Task

1 Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.

2 Click **Desktop Firewall**.

3 Click 🔒, type the administrator password, then click **OK**.

4 Select **Regular Mode**.

5 Click + in the bottom left corner of the console to create a firewall rule.

   a Type a name of the rule in the **Rule Name** text box.

   b Select **Enabled** from the **Status** drop-down list.

   c Select **Allow** from the **Action** drop-down list.

   d Select **Outgoing** from the **Direction** drop-down list.

6 In the **Network Protocol (IPv4)**, section:

   a Select **Any Local IP Address** for **Local**.

   b Click ⊕, select **Fully Qualified Domain Name** for **Remote**, then type the **Domain Name**.

7 In the **Transport Protocol** section, select **All Protocols**.

8 Open the browser, type the website name, then press **return**.

> Make sure no McAfee ePO rule allows access to this domain.

Uninstall the software

Remove the software from the standalone Mac and remove the software and its related extensions from the Mac that is managed by ePolicy Orchestrator.

Tasks

- *Uninstall the software from a standalone Mac* on page 26
  You can uninstall the software from a Mac using the command line.
- *Remove the software from a managed Mac* on page 27
  Remove McAfee Endpoint Protection for Mac from the managed Mac and remove the extensions from the ePolicy Orchestrator server.

Uninstall the software from a standalone Mac

You can uninstall the software from a Mac using the command line.

> **Before you begin**
>
> You must have administrator rights to uninstall the software.

Task

1 Open a Terminal window.

2 Type the following command, then press **return**.

```
sudo /usr/local/McAfee/uninstall EPM
```

> The uninstallation command is case sensitive.

3 Type the administrator password when prompted.

> When self-protection feature is enabled in **EndPoint Protection for Mac 2.1.0** | **General** | **General Policies**, uninstalling the software using the command line prompts you to type the password provided by the ePolicy Orchestrator administrator.

When the software is uninstalled, the following message appears:

McAfee Endpoint Protection for Mac 2.1.0 has been uninstalled successfully.

> When you uninstall the software, the McAfee Agent is not uninstalled from the system. This is because that it might be used by other products. Refer to the product guide of your McAfee Agent version for more information.

Remove the software from a managed Mac

Remove McAfee Endpoint Protection for Mac from the managed Mac and remove the extensions from the ePolicy Orchestrator server.

Tasks

- *Remove the software* on page 27
  Create a client task on the ePolicy Orchestrator to remove McAfee Endpoint Protection for Mac from the managed Mac.
- *Remove the software extensions* on page 28
  Remove the McAfee Endpoint Protection for Mac extensions from the ePolicy Orchestrator server.

Remove the software

Create a client task on the ePolicy Orchestrator to remove McAfee Endpoint Protection for Mac from the managed Mac.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. Click the **Assigned Client Tasks** tab, then click **New Client Task Assignment**.
4. Complete these options, then click **Create New Task**.
   a. For **Products**, select **McAfee Agent**.
   b. For **Task Type**, select **Product Deployment**.
5. On the **Client Task Catalog** page:
   a. Type a name for the task.
   b. Select **Mac** as the target platform.
   c. In **Products and components**, select **McAfee Endpoint Protection for Mac 2.1**, select **Remove** as action, then click **Save**.
6. On the **Client Task Assignment Builder** page:
   a. Select the task, then click **Next**.
   b. Schedule the task to run immediately. Click **Next** to view a summary of the task, then click **Save**.
7. In the **System Tree**, select the systems or groups for which you assigned the task, then click **Wake Up Agents**.
8. Select **Force complete policy and task update**, then click **OK**.

> When self-protection feature is enabled in **EndPoint Protection for Mac 2.1.0** | **General** | **General Policies**, uninstalling the software using the command line prompts you to type the password provided by the ePolicy Orchestrator administrator.

Remove the software extensions

Remove the McAfee Endpoint Protection for Mac extensions from the ePolicy Orchestrator server.

> ! Remove only the extensions for McAfee Endpoint Protection for Mac. Do not remove the Host Intrusion Prevention extensions because they are used by other products or systems.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Software** | **Extensions**.
3. In the left pane, select the extension and click **Remove**.
4. Select **Force removal, bypassing any checks or errors**, then click **OK**.

3 Using the software on a standalone Mac

You can use the McAfee Endpoint Protection for Mac console to view the dashboard, events details, the history of all events, quarantined items, and to configure scan schedules.

Contents

- *Dashboard*
- *History of events*
- *Quarantine malware*
- *Remove or restore the quarantined item*
- *Update the anti-malware and DAT files*
- *Perform a system scan*
- *Configure custom scan tasks*

Dashboard

The dashboard displays the security status of your Mac, malware detection statistics, version details of engine and DAT files, and recent events summary.

To view the dashboard, click the McAfee menulet on the status bar, select **McAfee Endpoint Protection for Mac Console**, then click **Dashboard**. The events that are listed in the dashboard are read-only.

Security status

View the security status and the protection features that are enabled or disabled on your Mac.

Use the dashboard to know the status of:

- **On-access Scan**
- **Spyware Scan**

- **Application Protection**
- **Desktop Firewall**

Recent events summary

You can view the summary of recent five events in **Dashboard**.

The events summary includes:

- Status of scan task with number of malware detected from on-access scan and on-demand scan.
- Anti-malware update status with DAT version details.
- Prevention of application execution details.

> **Recent events** displays only the summary of events. To view the complete details of events, navigate to the **History** page, then double-click the particular event.

History of events

The **History** page displays all events with details for virus and spyware scanning, anti-malware update, and blocked applications.

To view **History**, click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**. Twenty events are listed per page and you can use arrow keys to navigate through pages.

To...	Do this...
View events	Double-click the event you want to view. • **Anti-malware Update** — Displays the DAT version, engine version, and the status of the update. • **Blocked** — Displays the blocked application path. • **On-access Scan** — Displays the application that accessed the malware, status of detection found, and total number of detections with the details. • **On-demand Scan** — Displays number of files scanned, name and location of infected files, if found, and action taken.
Sort events	Click the column header to sort events based on title, type, or date and time.
Remove events	1 Click , type the administrator password, then click **OK**. 2 Select the event, then click **Delete**. 3 Click **OK** to remove the events. You can't restore the events once you remove them from the list. 4 Click to prevent further changes.

Quarantine malware

The quarantine feature isolates dangerous or suspicious malware that could harm your Mac otherwise.

To view the quarantined items, from the status bar, click the McAfee menulet | **McAfee Endpoint Protection for Mac Console** | **Quarantine**. The quarantine page displays the original path of items quarantined with date and time of the event. You can either remove or restore the quarantined item.

Remove or restore the quarantined item

The **Dashboard** displays the list of quarantined items with the path, date, and time. You can restore the quarantined items, only if you are sure that they are non-malicious items, otherwise you can remove them.

Before you begin

You must have administrator rights to remove or restore the quarantined item from the list.

> Before restoring an item, we recommend that you send it to McAfee Labs for testing. To submit a sample to McAfee Labs, see KB article 68030.

Task

1. Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**.
2. On the console dashboard, click **Quarantine**.
3. Click 🔒, type the administrator password, then click **OK**.
   - To restore, select the quarantined item, click **Restore**, then click **OK** to confirm.
   - To remove, select the quarantined item, click **Delete**, then click **OK** to confirm.
4. Click 🔓 to prevent further changes.

Update the anti-malware and DAT files

Always keep anti-malware and DAT files up to date to protect your Mac from the latest threats.

Task

1. Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**.
2. On the console dashboard, click **Update Now**.
3. Click **Start Update** to initiate the anti-malware update task.

Upon completion, the update summary appears with the engine version, DAT version, update status, and DAT creation date in the **Anti-malware Update** section. You can view the status and details of anti-malware update event in the **History** page.

> To schedule an automatic update, see *Configure anti-malware update schedule*.

Perform a system scan

Perform an on-demand scan on specific files, folders, and local or network-mounted volumes immediately.

Task

1. Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**.
2. On the console dashboard, click **Scan Now**.
3. From the **What to scan** drop-down list, select **Start Scan**.

Configure custom scan tasks

Schedule and customize scan tasks based on your requirements, to scan specific files, folders, and volumes periodically. You can also modify or remove the existing schedule.

For example, to scan your download folder and music library folder more frequently, you can define a scan schedule for only these two folders.

Tasks

- *Create a scan task* on page 32
  Create scan tasks that automatically run at scheduled periods with the defined parameters.
- *Modify an existing scan task* on page 33
  Modify an existing scan schedule to add or remove locations or change the date and time.
- *Remove an existing scan schedule* on page 33
  Remove the scheduled scan schedule when you no longer need it.

Create a scan task

Create scan tasks that automatically run at scheduled periods with the defined parameters.

Task

1. Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**.
2. On the console dashboard, click **Scan Now**.
3. Click + in the bottom left corner.
4. In the **Scan Name** field, type a name, then click **Create**.
5. From the **What to scan** drop-down list, select the items you want scan. Click + or - to remove the location.
   - **Documents** — Scans the user documents folder.
   - **Desktop** — Scans files and folders in desktop.
   - **Users** — Scans the user directory.
   - **Applications** — Scans the applications folders.
   - **Localhost** — Scans the local host.
   - **Choose** — Allows you to select folder or file location to scan.

6 In the **When to scan** section, select a schedule for the scan task, then click **Schedule Scan**.

- **Immediately** — Starts a scan task immediately. If you select to scan items **immediately**, click **Start Scan**.
- **Once** — Scans the defined locations once at the scheduled date and time.
- **Daily** — Scans the defined locations every day at the scheduled time. You can define the duration to run the daily scan task or select **No End Date** to run the schedule without any limit.
- **Weekly** — Scans the defined locations on a scheduled day and time of every week. You can define the duration to run the weekly scan task or select **No End Date** to run the schedule without any limit.
- **Monthly** — Scans the defined locations on a scheduled date and time of every month. You can define the duration or select **No End Date** to continue the schedule without any limit.

7 When you see a message that the scan task is scheduled, click **OK**.

Modify an existing scan task

Modify an existing scan schedule to add or remove locations or change the date and time.

Task

1 Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**.

2 On the console dashboard under **Activity**, click the schedule you want to modify. The schedule displays the **Last Scan Time** and **Next Scan Schedule**.

3 Click **Modify Scan**, make the needed changes, then click **Schedule Scan**.

> To run the scan schedule immediately, select the scan, make the needed changes, then click **Schedule Scan**.

Remove an existing scan schedule

Remove the scheduled scan schedule when you no longer need it.

Task

1 Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Console**.

2 On the console dashboard, select an existing scan schedule in the left pane.

3 In the bottom left corner of the console, click − to remove the selected item.

4 Configuring protection preferences on a standalone Mac

Use McAfee Endpoint Protection for Mac preferences to enable or disable anti-malware, application protection, desktop firewall, and to configure the protection parameters.

Contents

- *General preferences*
- *Anti-malware*
- *Application protection*
- *Desktop firewall*
- *Configure an update schedule*

General preferences

Enable or disable the protection features that you want to run on your Mac.

Configure general preferences

Enable or disable the security features you want to configure for your Mac.

Before you begin

You must have administrator rights to configure these protection preferences.

Task

1. Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. On the **General** tab, click , type the administrator password, then click **OK**.
3. Click **ON** or **OFF** to enable or disable these features:
   - **On-access Scan** — Detects malware, whenever a file is read from or written to the hard disk.
   - **Spyware Scan** — Detects spyware and takes preventive actions.

- **Application Protection** — Define rules for applications, to run with full network access, restricted network access, or deny application execution.
- **Desktop Firewall** — Define rules that control incoming and outgoing network traffic.

4. Click 🔓 to prevent further changes.

> McAfee Endpoint Protection for Mac is shipped with the default set of policies. Verify the protection preferences for each component and make sure that it matches your requirements.. For more information on setting preferences, see *Configure protection preferences*.

Anti-malware

Configure anti-malware preferences to define the actions for an on-access scan or on-demand scan, and to exclude specific paths from scanning.

Configure on-access scan preferences

The on-access scan protects your Mac from threats in real time. It scans for malware whenever an item is read from or written to the hard disk, and cleans or quarantines the file according to your configuration.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. On the **Anti-malware** tab, click 🔒, type the administrator password, then click **OK**.
3. From the **Scan files while** drop-down list, select one of these options:
    - **Read** — To scan items When they are read from the hard disk.
    - **Write** — To scan items when they are written to the hard disk.
    - **Read & Write** — To scan items when they are read from or written to the hard disk.
4. In **Maximum scan time (in seconds)**, specify the duration allowed to scan each file. You can specify a value between 10 and 999. The default value is 45.
5. From the **When a virus is found** drop-down list, select one of these options:
    - **Clean** — To clean the item that contains a virus. Use the **If clean fails** drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
    - **Quarantine** — To quarantine the item that contains a virus. Use the **If clean fails** drop-down list, to select a secondary action (delete the item or send notification)
    - **Delete** — To delete the item that contains a virus.
    - **Notify** — To notify you when a virus is detected. No other action is taken.
6. From the **When a spyware is found** drop-down list, select one of these options:
    - **Clean** — To clean the item that contains spyware. Use the **If clean fails** drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
    - **Quarantine** — To quarantine the item that contains spyware. Use the **If clean fails** drop-down list, to select a secondary action (delete the item or send notification)

- **Delete** — To delete the item that contains spyware.
- **Notify** — To notify you when spyware is detected. No other action is taken.

7 From the **Also scan** drop-down list, select where you want to enable scanning:

- **Archives & Compressed Files**
- **Apple Mail Messages**
- **Network Volumes**

> When these options are selected, McAfee Endpoint Protection for Mac will detect the threat. But, the primary and secondary actions may vary depending on the options selected. For more information, see KB article 78277

8 Click 🔓 to prevent further changes.

Configure on-demand scan preferences

Schedule an on-demand scan to run immediately, at a scheduled time, or at regular intervals.

> For information on creating a scan task, see *Create a scan task*.

Task

1 Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.

2 On the **Anti-malware** tab, click **On-demand Scan**.

3 Click 🔒, type the administrator password, then click **OK** to open the **On-demand scan** page.

4 From the **When a virus is found** drop-down list, select one of these options:

- **Clean** — To clean the item that contains a virus. Use the **If clean fails** drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
- **Quarantine** — To quarantine the item that contains a virus. Use the **If clean fails** drop-down list, to select a secondary action (delete the item or send notification)
- **Delete** — To delete the item that contains a virus.
- **Notify** — To notify you when a virus is detected. No other action is taken.

5 From the **When a spyware is found** drop-down, select one of these options:

- **Clean** — To clean the item that contains spyware. Use the **If clean fails** drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
- **Quarantine** — To quarantine the item that contains spyware. Use the **If clean fails** drop-down list, to select a secondary action (delete the item or send notification)
- **Delete** — To delete the item that contains spyware.
- **Notify** — To notify you when spyware is detected. No other action is taken.

6. From the **Also scan** drop-down list, select where you want to enable scanning:
   - **Archives & Compressed Files**
   - **Apple Mail Messages**
   - **Network Volumes**

   > When you run a full scan, by default, all network volumes mounted on your Mac are scanned for threats.

7. Click 🔓 to prevent further changes.

Define anti-malware exclusions

Exclude files and folder paths from an on-access scan or on-demand scan.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. Click **Anti-malware**, then click **Exclusions**.
3. Click 🔒, type the administrator password, then click **OK**.
4. Click + in the bottom left corner of the console.
5. Select the path of the required files and folders, then click **Open**.
6. Select or deselect the **On-access Scan** and **On-demand Scan** options as needed.
   - Double-click an item to change the name or path that appears in the exclusion list.
   - Use regular expressions to exclude items from scanning. For example, to exclude all files in the desktop from scanning, specify the path as /Users/user/Desktop/*.*
   - To remove the item from the exclusions list, select it, then click − in the bottom left corner of the page (or press **fn**+**delete**).

   > If you deselect the **On-access Scan** and **On-demand Scan** options for a path added to the exclusion list, the path is removed from the exclusion list immediately.

7. Click 🔓 to prevent further changes.

Best practices for anti-malware preferences

This section describes the best practices to define the preferences for scheduling on-access scan and on-demand scan.

On-access scan preferences

- Always enable **On-access-Scan** because it checks every file the user accesses, and detects malware before it runs.
- Enable the scan option for the **Network Volumes** when needed, to scan files copied from or written to any network volumes.
- Always select **Quarantine** as the secondary action for virus and spyware detections so that you can retrieve the files from the product console later.

On-demand scan preferences

- Always enable the scan for **Archives & Compressed Files** while performing on-demand scan. This is recommended because you may have disabled scanning option for these files.
- Always select **Quarantine** as the secondary action for virus and spyware detections so that you can retrieve the files from the product console later.

On-demand scan schedule

- Schedule an on-demand scan during non-peak hours (for example, during weekends or maintenance period).
- When scheduling an on-demand scan for the first time, schedule a full on-demand scan of your entire hard disk.

Anti-malware exclusions

You can add regular expressions that match required patterns to exclude multiple files and folders from being scanned.

Here are some recommended exclusions:

- Microsoft Outlook database files
- Thunderbird database files
- Encrypted files
- Generic plist files such as `Info.plist` or `version.plist` for on-access scanning

Here are the regular expressions for some of the recommended exclusions:

- To exclude files with the extension mdb, use .*\.mdb.
- To exclude files with the extension mdb or odc, use .*\.(mdb|odc.
- To exclude each user's Entourage/Outlook Database files of different Microsoft Office version, use /Users/.*/Documents/Microsoft\ User\ Data/Office\ \d+\ Identities/.*Identity/Database.
- To exclude all Info.plist, version.plist under /Applications, use /Applications/.*/Contents/(version|Info).plist.
- To exclude files with the extensions jar, rar, or war under /private/var/tmp, use /private/var/tmp/.*\..+ar.
- To exclude files under /private/var/tmp starting with a letter and ending with a number, use /private/var/tmp/([A-Z]|[a-z]).*[0-9]$.

Application protection

Application protection allows you define rules to run applications without restrictions, with restrictions, or block the execution.

Configure preferences for application protection

Define the permission preferences for Apple-signed binaries and modified or unknown applications.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. On the **Application Protection** tab, click 🔒, type the administrator password, then click **OK**.

3. On the **Rules** tab, you can:
   - Select or deselect **Allow All Apple Signed Binaries**.
   - Select **Allow**, **Deny**, or **Prompt** from the **Unknown/Modified Applications** drop-down list to configure application execution and network access settings for unknown and modified applications.

   If you select **Prompt**, type <n> seconds (where n is a value between 10 and 300). The **McAfee Alert** page appears for <n> seconds, prompting you to select an action for the application as **Always** or **Once**, with these options:
   - **Allow Execution with Full Network Access** — Executes the application with full network access.
   - **Allow Execution without Network Access** — Executes the application without network access.
   - **Deny Execution** — Blocks the application execution.

   ⚠ If you do not respond to the **McAfee Alert**, the execution is denied for the selected application.

4. Click 🔓 to prevent further changes.

Create an application protection rule

Rules determine whether the application can be executed or blocked, and if executed, whether it can run with full, restricted, or no network access.

Task

1. Click the McAfee menulet 🛡 on the status bar, select **McAfee Endpoint Protection for Mac Preferences**, then click the **Application Protection** tab.
2. Click 🔒, type the administrator password, then click **OK**.
3. Click + in the bottom left corner of the console.
4. In **Application Name**, click 🔍, then select the application.
5. In **Action**, select one of these options:
   - **Allow Execution With Full Network Access**
   - **Allow Execution Without Network Access**
   - **Allow Execution With Restricted Network Access**
   - **Deny Execution**
6. If you select **Allow Execution With Restricted Network Access**, define these protocols. Click + in the bottom left corner of the console to add:
   - **Protocol**
   - **IP Address/Subnet**
   - **Port/Range**
   - **Direction**
   - **Action**
7. Click **OK** to return to the **Rules** page.
8. Click 🔓 to prevent further changes.

Modify an existing application protection rule

You can modify the existing application protection rule's definition that is in force, according to your requirement.

Task

1 Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.

2 On the **Application Protection** tab, click 🔒, type the administrator password, then click **OK**.

3 Double-click the rule you want to modify, make the needed changes, then click **OK** to return to the **Rules** page.

> To delete a rule, select it and click -, or press **fn** + **delete**.

4 Click 🔓 to prevent further changes.

Reapply rules for modified applications

Reapply the existing protection rules for applications or binaries that are modified or updated.

Whenever there is a change in the application or binary due to updates, the corresponding application protection rules become invalid.

Consider a scenario where you have set a rule as **Allow Application to Run with Restricted Network Access** for Safari. When you run the updates for Safari manually or automatically, the defined rules for Safari become invalid. You must reapply the rules after completing the update.

Task

1 Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.

2 Click 🔒, type the administrator password, then click **OK**.

> When you select a rule for the updated application, the reapply button becomes active.

3 From the list of rules, select the rule for the application that was updated, then click √.

The rules for modified applications or binaries are reinstated.

4 Click 🔓 to prevent further changes.

Specify exclusions for application protection

Exclude trusted applications from the application protection rules. This option overrides any application protection rules you created already.

Task

1 Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.

2 On the **Application Protection** tab, click **Exclusions**.

3 Click 🔒, type the administrator password, then click **OK**.

4 Click + in the bottom left corner of the page.

5. From the list, add the path of the applications you want to exclude, then click **Open**.
6. Click 🔓 to prevent further changes.

   > To delete an exclusion, select the item, then press **fn**+**delete**.

Best practices for application protection

We recommend that you follow this strategy to configure application protection rules that match your business needs.

Administrators can create clear rules to allow only authorized applications are allowed to execute with the defined privileges.

We recommend that you run the application protection configuration on a test environment, before applying it on production systems.

1. Based on your organization's policy, identify the applications:
   - That are vulnerable but need protection.
   - That caused a security compromise recently.
   - That you want to block from execution.
2. Create a test environment in your lab with real-time applications. You can also include a few real-time users and systems as part of testing.
3. Prepare a list of applications you want to allow, block, or run with restricted network access. We recommend that initially you create basic rules. Refer to this sample checklist for your environment:

Application	Execution permission	Network access
Safari	Yes	Unrestricted
iTunes	Yes	No network
Messenger	No	No network
Firefox	Yes	Unrestricted
iChat	Yes	Restricted (No external access)

4. Observe the system behavior and performance for a week and monitor the events regularly during the test run. Monitoring includes checking the behavior and impact on normal operations, as a result of application protection rules, application updates, and any new applications that the user installed.

   Check the update or upgrade of applications that are associated with application protection rules.

   For example, you have added a rule for Safari. When you upgrade this application to the next version (major or minor), the updated version is treated as an unknown or modified application. In this case, appropriate action takes place based on the settings configured for the unknown or modified application. We recommend that you update your rules.

   Whenever an update or upgrade takes place for applications, re-apply the associated rules after the application update or upgrade.

Recommended application protection configuration

- Add basic rules to allow or block certain applications based on the checklist prepared earlier. During this stage, do not add any rules for restricted network access or advanced rules for certain binaries.
- Verify and make sure that no third-party application protection and firewall products are installed on the systems that are being used in the test environment.
- Notify users that they are receiving new protection and provide solution steps wherever required.
- Add rules for Apple-specific applications and binaries to block their execution and network access.
- Reapply the rules, whenever the application is updated or upgraded in standalone mode. When the system is managed by ePolicy Orchestrator, rules are automatically re-applied when the next policy enforcement occurs.
- While adding rules for applications that are dependent on binaries in different folders, also add rules for dependent binaries.

Desktop firewall

The desktop firewall component provides a scalable solution to protect your Mac from unauthorized network traffic.

The firewall comes with a stateful engine that provides flexibility in defining allowed network traffic for your Mac. You can define rules based on various traffic parameters and group them for easier management.

Here is the list of features of desktop firewall protection:

- **Stateful filtering** — The stateful filtering and network packet inspection validate each packet for different connections against predefined rules, holding the connection attributes in memory from beginning-to-end.
- **Regular mode** — When the network packet adheres to a rule's condition, the associated action defined in the rule is executed. If no matching rule is found, the network packet is blocked.
- **Adaptive mode** — When the network packet matches a rule's conditions, the associated action defined in the rule is executed. If no matching rule is found, the network packet is allowed and a rule is created to allow similar packets later. Use this option to fine tune your firewall rules.

  In both these modes, the status of the TCP/UDP/ICMP connection is tracked to identify whether the incoming packet is part of the existing connection.

- **New rules and grouping rules** — You can create rules and group them for easier management.
- **DNS blocking** — Blocks access to unwanted domains.
- **Location awareness** — Creates separate rules for locations, such as office or home network.

- **FTP inspection** — Desktop firewall automatically creates dynamic rules for FTP data connections, by actively monitoring the FTP commands on the control channel.
- **Trusted networks** — You can define networks that can include subnets, ranges, or a single IP address that can be used while creating firewall rules.

> McAfee recommends you to use ePolicy Orchestrator for managing firewall, so that you can avail various features such as, location awareness, trusted networks, DNS blocking, and rules grouping. These features are available only through McAfee ePO.

How stateful filtering works

Stateful filtering preserves in memory the list of existing network connections allowed by the firewall. Each entry in the state table contains multiple parameters that help to identify the connection state.

When the network packet finds an allow rule, the packet is allowed and a new entry is added to the state table. The subsequent packets are allowed without further verification of the predefined rule sets. When the session is completed or timed out, the entry is removed from the state table.

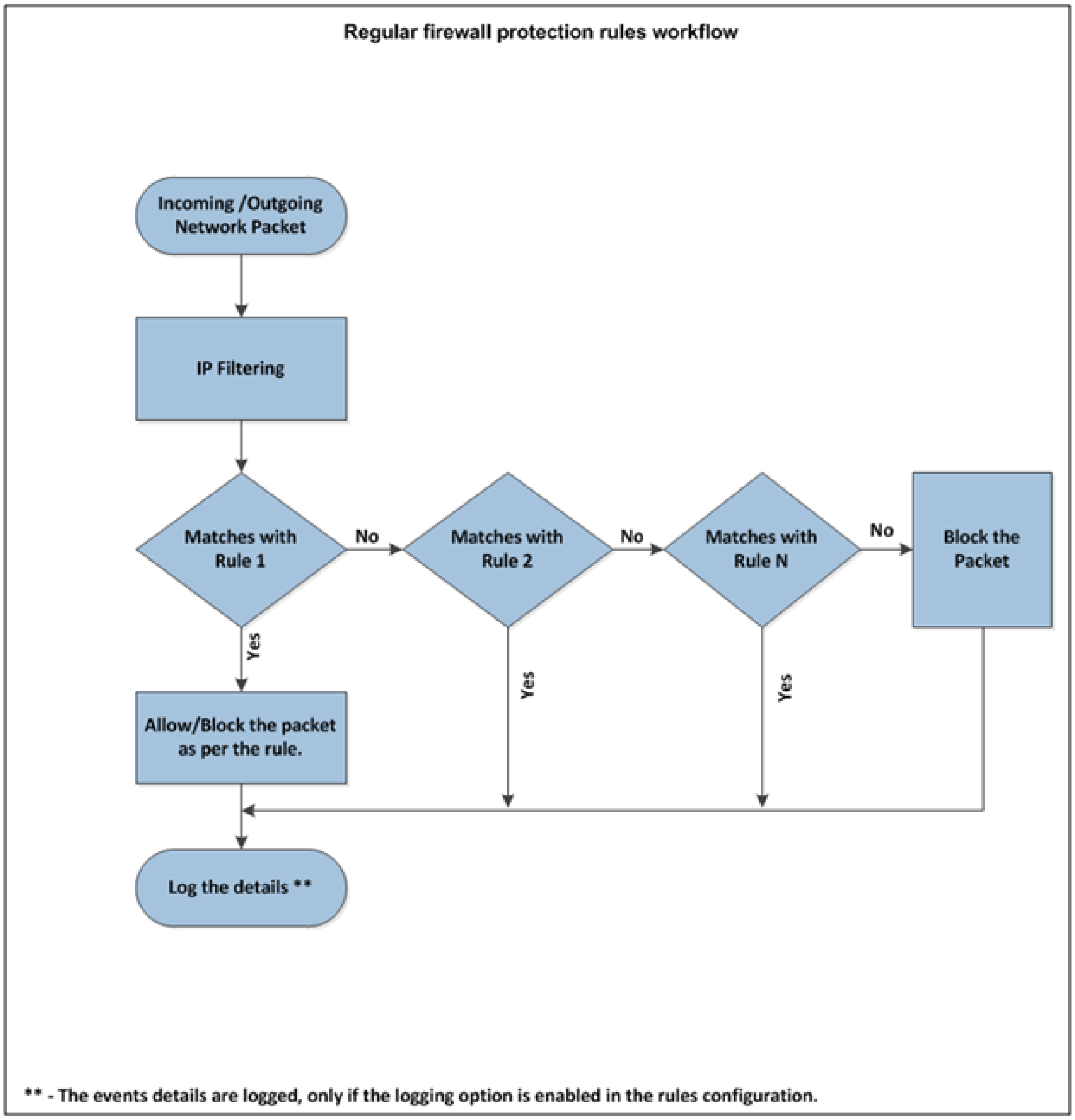
Stateful filtering automatically tracks the reverse traffic for existing connections eliminating the need for another firewall rule. Desktop firewall performs stateful filtering on TCP, UDP, and ICMP protocols.

How regular mode firewall protection works

Each rule contains a set of conditions that the network traffic must meet. The associated parameters of that rule allow or block the network traffic.

In Regular mode, desktop firewall uses precedence to apply rules. The rule at the top of the rules list is applied first. If the network packet meets the conditions, desktop firewall allows or blocks the packet as defined. If the packet does not meet the first rule's condition, the next rule is verified and moves through the rules list until a rule is satisfied. If no rule is met from the rules list, desktop firewall blocks the traffic.

When the traffic matches the rule condition, desktop firewall does not try to apply any further rules from the list.


Regular firewall protection rules workflow
Incoming /Outgoing Network Packet
IP Filtering
Matches with Rule 1
No
Matches with Rule 2
No
Matches with Rule N
No
Block the Packet
Yes
Yes
Yes
Allow/Block the packet as per the rule.
Log the details **
** - The events details are logged, only if the logging option is enabled in the rules configuration.

To change the desktop firewall protection from Regular mode to Adaptive mode, click | **McAfee Endpoint Protection for Mac Preferences** | **Desktop Firewall** | **Adaptive Mode**.

How Adaptive mode firewall protection works

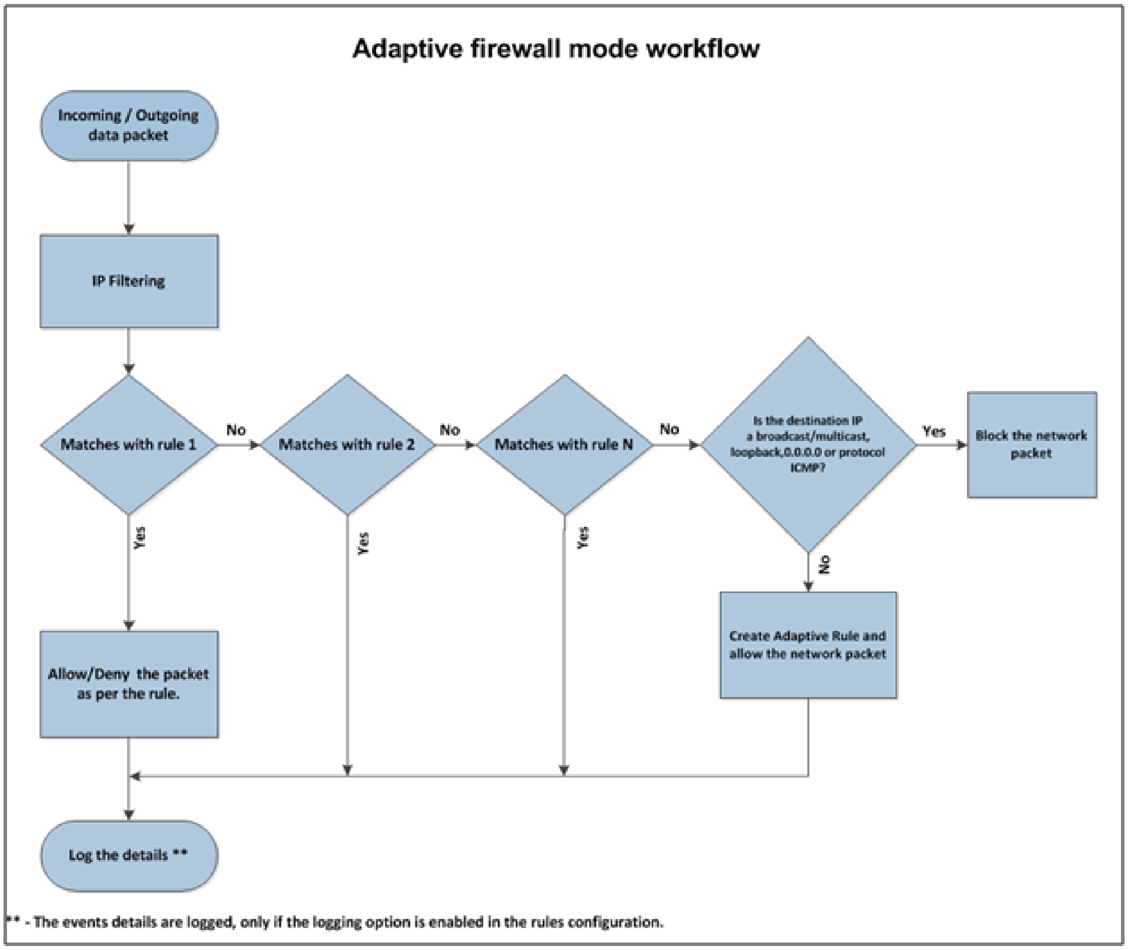
In Adaptive mode, the precedence method is followed, but differently than in Regular mode.

In Adaptive mode, desktop firewall uses precedence to apply rules. The rule at the top of the rules list is applied first. When the network packet does not match the defined rules from the list, an allow rule is created to allow the non-matching packet.

If the IP destination is a broadcast, multicast, loopback, or ICMP protocol, the network packet is blocked.

For security reasons, when Adaptive mode is enabled, incoming pings are blocked unless an explicit allow rule is created for incoming ICMP traffic.

This diagram shows how network packets are handled in Adaptive mode.


Adaptive firewall mode workflow

Incoming / Outgoing data packet
IP Filtering
Matches with rule 1
No
Matches with rule 2
No
Matches with rule N
No
Is the destination IP a broadcast/multicast, loopback,0.0.0.0 or protocol ICMP?
Yes
Block the network packet
Yes
Yes
Yes
No
Allow/Deny the packet as per the rule.
Create Adaptive Rule and allow the network packet
Log the details **

** - The events details are logged, only if the logging option is enabled in the rules configuration.

To change the desktop firewall protection from Adaptive mode to Regular mode, click | **McAfee Endpoint Protection for Mac Preferences** | **Desktop Firewall** | **Regular Mode**.

How DNS blocking works

You can create a list of domain names for which you want to block access.

Specify the domain names that you want to block. You can use ? and * wildcards to define the domain names.

> If the firewall host has not initiated any DNS queries for the blocked domains or FQDN, the DNS blocking and FQDN-based rules do not work.

How stateful FTP inspection works

Desktop firewall can perform stateful inspection for the FTP protocol.

FTP involves two connections:

- Control for commands
- Data for the information

When a client connects to an FTP server, the control channel is established on FTP destination Port 21, and an entry is made in the state table. If the option for FTP inspection was set with the Firewall Options policy, when the firewall encounters a connection opened on Port 21, it knows to perform stateful packet inspection on the packets coming through the FTP control channel.

Desktop firewall monitors the `PORT`, `EPRT`, `PASV`, and `EPSV` commands on the control channel, and determines which dynamic rules must be created for subsequent FTP data connections.

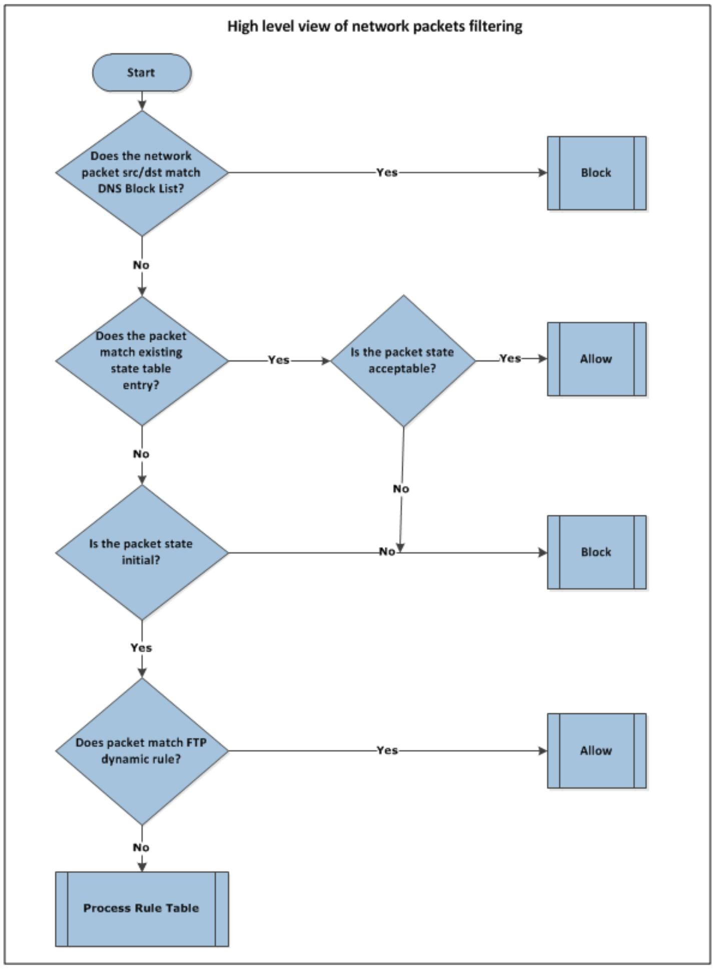
The combination of the control connection and one or more data connections is called a *session*. When the data transfer is complete, the dynamic rules created for data transfer are removed.

When the control connection is terminated, desktop firewall makes sure that all corresponding data connections are also removed.

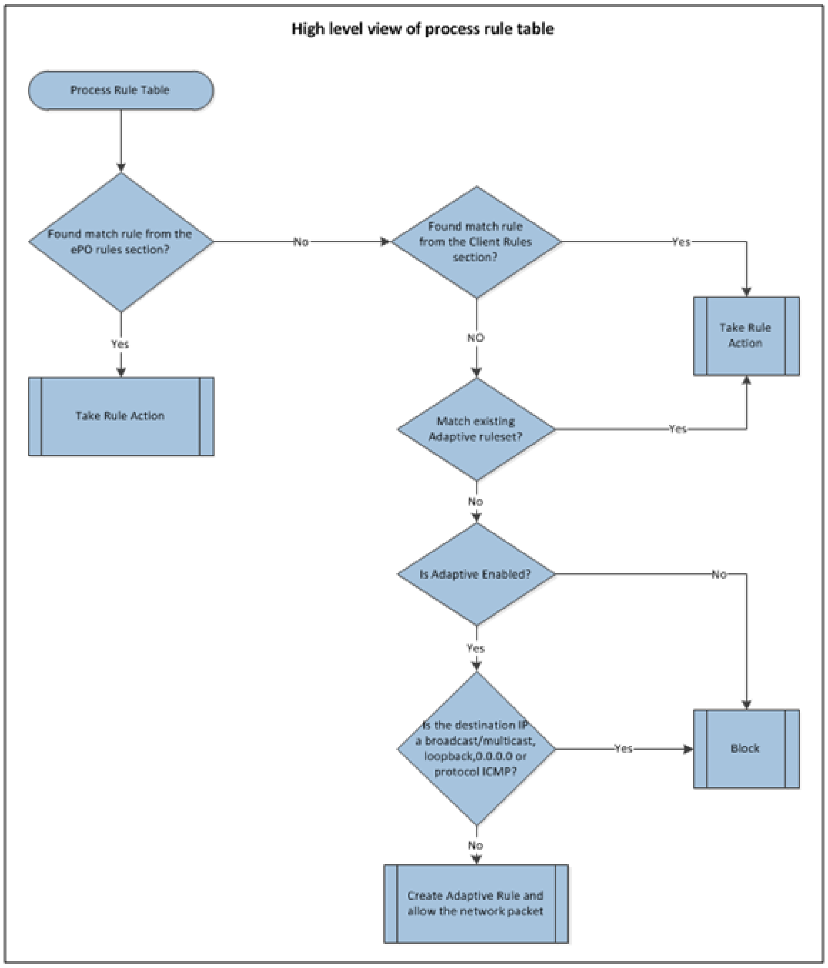
How desktop firewall rules work

Each rule contains a set of conditions that the network traffic must meet. The associated parameters of that rule allow or block the network traffic.

This diagram shows how network packet filtering works.


High level view of network packets filtering
Start
Does the network packet src/dst match DNS Block List?
Yes
Block
No
Does the packet match existing state table entry?
Yes
Is the packet state acceptable?
Yes
Allow
No
No
Is the packet state initial?
No
Block
Yes
Does packet match FTP dynamic rule?
Yes
Allow
No
Process Rule Table

This diagram explains how the process rule table flow works for each network packet.


High level view of process rule table
Process Rule Table
Found match rule from the ePO rules section?
No
Found match rule from the Client Rules section?
Yes
Take Rule Action
Yes
NO
Take Rule Action
Match existing Adaptive ruleset?
Yes
No
Is Adaptive Enabled?
No
Yes
Is the destination IP a broadcast/multicast, loopback,0.0.0.0 or protocol ICMP?
Yes
Block
No
Create Adaptive Rule and allow the network packet

How desktop firewall rules are organized

Rules are categorized as **ePO Rules**, **Client Rules**, and **Adaptive Rules**.

Rules are displayed in tree view. The **ePO Rules** group appears at the top with the list of rules, followed by the **Client Rules**, then the **Adaptive Rules**.

To view desktop firewall rules, click | **McAfee Endpoint Protection for Mac Preferences** | **Desktop Firewall**.

- **ePO Rules** — Defined and enforced by administrators if your Mac is managed by ePolicy Orchestrator.

  The **ePO Rules** group contains list of rules that desktop firewall creates automatically at run time. These rules can't be modified.

  - **ePO Rules** are displayed and applied only when the Mac is managed by ePolicy Orchestrator.
  - A local user can't modify **ePO Rules**.
  - A user can't add rules above or in between **ePO Rules**.
  - When rules are created from a client Mac, they are added after the existing rules in the respective group.
  - These are the first rules processed to match the network packet.

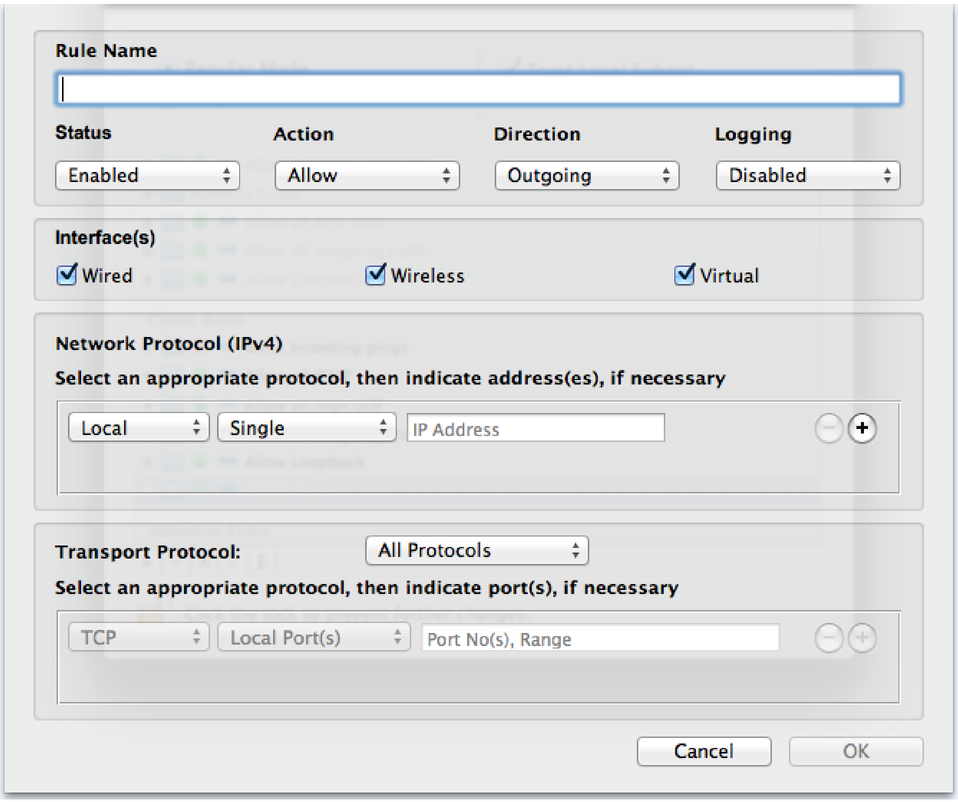
- These rules allow the Mac to:
  - Obtain an IP address using DHCP.
  - Perform DNS queries.
  - Perform DAT updates.
  - Allow communication with ePolicy Orchestrator.
- **Client Rules** — Created locally to allow or block specific network access.
- **Adaptive Rules** — Created automatically to allow the packet whenever a non-matching data packet is received.

Create a firewall rule

Add specific rules at the top of the list, and generic rules at the bottom to filter the traffic most efficiently.

Task

1. Click the McAfee menulet on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. Click **Desktop Firewall**.
3. Click 🔒, type the administrator password, then click **OK**.
4. Select **Regular Mode**.
5. Click + in the bottom left corner of the console to open the rule page.



Rule Name

Status: Enabled
Action: Allow
Direction: Outgoing
Logging: Disabled

Interface(s)
☑ Wired ☑ Wireless ☑ Virtual

Network Protocol (IPv4)
Select an appropriate protocol, then indicate address(es), if necessary
Local | Single | IP Address

Transport Protocol: All Protocols
Select an appropriate protocol, then indicate port(s), if necessary
TCP | Local Port(s) | Port No(s), Range

6. Define the following parameters as needed, then click **OK**.

For this field...	Configure these options...
Rule Name	Type a name for the rule.
Status	• **Enabled** — To enable the firewall rule. • **Disabled** — To disable the firewall rule. The rules appear as greyed out in the rules list, when it's status is set to **Disabled**.
Action	• **Block** — To block the network traffic. • **Allow** — To allow the network traffic.
Direction	• **Incoming** — To apply the rules for incoming network traffic. • **Outgoing** — To apply the rules for outgoing network traffic.
Logging	• **Enabled** — To create an event log. • **Disabled** — To avoid creating an event log. Enabling the logging feature may impact the system performance. We recommend that you enable Logging only for troubleshooting and learning purpose.
Interface(s)	• **Wired** • **Wireless** • **Virtual**

For this field...	Configure these options...
Network Protocol IPv4	Define the configuration for **Local** Mac using: • **Single** • **Subnet** • **Local Subnet** • **Range** (of IP addresses) • **Fully Qualified Domain Name** • **Any Local IP Address** • **Any IPv4 Address** Local system is the system on which you are adding rules. Select the configuration for **Remote** system using: • **Single** • **Subnet** • **Local Subnet** • **Range** (of IP addresses) • **Fully Qualified Domain Name** • **Any Local IP Address** • **Any IPv4 Address** Remote system is the system you want to connect. Use ⊕ to add more criteria and ⊖ to remove existing criteria.
Transport Protocol	Select **All Protocols** to apply the rule for all protocols. For **Select Protocol**, define the parameters for: • **TCP** • **UDP** • **ICMP** Use ⊕ to add more criteria and ⊖ to remove existing criteria.

7 Click 🔓 to prevent further changes.

> To edit an existing firewall rule, select the rule, then click E to open the rule page.

Desktop firewall rules examples

Use these examples for common scenario-based firewall rules to create firewall rules.

Create a rule to allow DHCP outgoing on UDP local port 68 to remote port 67

To create a firewall rule that allows you to get an IP address on an interface, and we recommend creating two rules. First create a rule to allow DHCP outgoing on UDP local port 68 and remote port 67, then create a rule to allow DNS queries.

- **Rule Name** — Type a name for the rule
- **Status** — Enabled
- **Network Protocol (IPv4)** — Not applicable
- **Transport Protocol** — Select **Protocol**

- **Action** — Allow
- **Direction** — Outgoing
- Select **UDP**, **Local**, then type the **Port No** as `68`
- Select **UDP**, **Remote**, then type the **Port No** as `67`

Create a rule to allow DNS queries

- **Rule Name** — Type a name for the rule
- **Status** — Enabled
- **Action** — Allow
- **Direction** — Outgoing
- **Network Protocol (IPv4)** — Not applicable
- **Transport Protocol** — Select **Protocol**
- Select **UDP**, **Remote**, then type the **Port No** as `53`

Create a rule to allow access to websites

- **Rule Name** — Type a name for the rule
- **Status** — Enabled
- **Action** — Allow
- **Direction** — Outgoing
- **Network Protocol (IPv4)** — Not applicable.
- **Transport Protocol** — Select **Protocol**
- Select **TCP**, **Remote**, then type the **Port No** as `80`

Allow specific remote IP address and port access

- **Rule Name** — Type a name for the rule
- **Status** — Enabled
- **Action** — Allow
- **Direction** — Outgoing
- In **Network Protocol (IPv4)**, select **Remote** | **Subnet**, then type the **Subnet Mask value**
- **Transport Protocol** — Select **Protocol**
- Select **TCP**, **Remote**, then type the **Port No**

You can type a single port number, or series of port numbers using a comma, or a range of ports using a hyphen.

Recommended firewall rules

In addition to the default firewall rules, we recommend that you configure these rules:

- Allow bi-directional NTP port 123 to 123
- Allow bi-directional NetBIOS name service port 137 to 137
- Allow outgoing FTP client port 1024-65535 to 21

- Allow outgoing for POP3, IMAP, SMTP
- Allow outgoing for RDP
- Allow outgoing for Idap
- Allow bi-directional for AFP/SMB, if you are using file sharing

Best practices for desktop firewall

We recommend that you configure these firewall rules that protect your system in line with your organizational requirements.

- McAfee Endpoint Protection for Mac is shipped with a set of default firewall rules. We recommend that you use them as starting point, and modify them according to your organizational requirements.
- If your organization does not have a firewall policy or if this is the first time your organization uses a firewall policy, we recommend that you use the default corporate policy. After, you can use the Adaptive mode for further fine tuning.

  ! We strongly suggest not to run Adaptive mode in production.

- Remember that Adaptive mode must be used to fine-tune the firewall rule sets. So, run Adaptive mode only for short duration to identify the organizational requirements.
- Define Trusted Networks so that you re-use it within rules.
- Configure the DNS blocking feature to block the known unwanted domains.
- Enable the FTP inspection.
- Always use firewall rule groups to organize the rules in an efficient way.
- Make rules as specific as possible.

  For example, to allow access to a particular website, provide the name or IP address, with the port number.

- Use more specific rules on the top of the rules set and the generic one toward the end.

  For example, to give access to a particular website for all Mac users in the organization except one system, create a specific deny rule to block the website on that particular system first.

- Because desktop firewall validates rules using a top-down approach, we recommend that you always revisit the rules completely to avoid the loopholes.

Configure an update schedule

Configure the repository list that needs to be accessed to update the anti-malware, the proxy connection settings, and the anti-malware update schedule.

Tasks

- *Configure the repository list* on page 54
  Always keep your DAT files and anti-malware up to date to secure your Mac from the latest threats.
- *Configure proxy settings* on page 54
  Configure **Proxy settings** if you use proxy servers to connect to the Internet for retrieving packages.
- *Configure the anti-malware update schedule* on page 55
  Periodic updates of anti-malware secure your Mac from latest threats.

Configure the repository list

Always keep your DAT files and anti-malware up to date to secure your Mac from the latest threats.

The software is shipped with the configuration that allows access to the McAfee FTP server, HTTP server, and the local repository to download the latest DAT files while your Mac is connected to the Internet.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. Click **Update**.
3. Click 🔒, type the administrator password, then click **OK**.
4. In **Repository Name** list box, on the **Repository List** tab:
   - + — To add a repository.
   - − — To delete an existing repository.
   - v — To prioritize repositories.
5. In **Repository Type**, select **FTP**, **HTTP**, or a **Local** repository from where the latest DATs can be downloaded.
6. Specify a **Repository URL**, **Port**, **User Name**, and **Password** for the repository.
7. On the **Schedule** tab, schedule the task, then click **Apply**.
8. Click 🔓 to prevent further changes.

Configure proxy settings

Configure **Proxy settings** if you use proxy servers to connect to the Internet for retrieving packages.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. Click **Update**, then click the **Proxy Settings** tab.
3. Click 🔒, type the administrator password, then click **OK**.

4. Select whether to use a proxy.
   - **Do not use a proxy**
   - **Configure proxy settings manually**
5. Select **Use these settings for all proxy types** to specify the same IP address and port number for all proxy types.
6. Select **FTP** or **HTTP** server, then type the IP address and port number of the selected server.
7. Select **Use authentication**, then type the user name and password for FTP, HTTP, or a local repository.
8. To bypass a proxy server for specific domains, select the **Specify exceptions**, then type the proxy server name.
9. Click 🔓 to prevent further changes.

Configure the anti-malware update schedule

Periodic updates of anti-malware secure your Mac from latest threats.

Task

1. Click the McAfee menulet 🛡 on the status bar, then select **McAfee Endpoint Protection for Mac Preferences**.
2. On the **Update** tab, click **Schedule**.
3. Click 🔒, type the administrator password, then click **OK**.
4. Click the drop-down list to select the update frequency, then click **Apply**.
   - **Never** — To never update anti-malware.
   - **Hourly** — To update anti-malware on hourly basis, then select the hours.
   - **Daily** — To update anti-malware daily, then type the time.
   - **Weekly** — To update anti-malware weekly, select weekdays, then type the time.
   - **Monthly** — To update anti-malware monthly, select the day of the month, then type the time.
5. Click 🔓 to prevent further changes.

5

Managing the software with ePolicy Orchestrator

Integrate and manage McAfee Endpoint Protection for Mac using ePolicy Orchestrator management software.

McAfee ePolicy Orchestrator provides a scalable platform for centralized policy management and enforcement on your McAfee security products and the systems where they are installed. It also provides comprehensive reporting and product deployment capabilities through a single point of control.

For instructions about setting up and using ePolicy Orchestrator and McAfee Agent, see the product guide for your version of each product.

Contents

- *Manage policies*
- *Create a self-protection policy*
- *Create an anti-malware policy*
- *Schedule an anti-malware update*
- *Schedule an on-demand scan*
- *Create an application protection policy*
- *Desktop firewall policy*
- *Create a DNS blocking policy*
- *Create a trusted networks policy*
- *Create a location awareness policy*
- *Queries and reports*

Manage policies

McAfee Endpoint Protection for Mac policies provide options to configure the features, feature administration, and to log details on a managed Mac.

You can find these policies on the **Policy Catalog** page under **Product**:

- **Endpoint Protection for Mac 2.1.0:Anti-malware**
- **Endpoint Protection for Mac 2.1.0:General**
- **Endpoint Protection for Mac 2.1.0:Application Protection**
- **Host Intrusion Prevention 8.0: Firewall**
- **Host Intrusion Prevention 8.0: General**
- **McAfee Agent**

Configure these policies with your preferences, then assign them to groups of the managed Mac. For generic information about policies, see the product guide for your version of ePolicy Orchestrator.

Tasks

- *Create or modify policies* on page 58
  You can create and edit policies for a specific group in the **System Tree**.
- *Assign policies* on page 58
  When you have created or modified policies, assign them to the systems that are managed by ePolicy Orchestrator.

Create or modify policies

You can create and edit policies for a specific group in the **System Tree**.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. From the **Policy Catalog**, select a **Product** and **Category**.
3. Perform these steps to create or modify a policy.

To create a policy	To modify a policy
1 Click **New Policy**. 2 Type the **Policy Name**. 3 Click **OK**. 4 Configure the settings.	1 Click the policy you want to modify. 2 Modify the settings.

4. Click **Save**.

Assign policies

When you have created or modified policies, assign them to the systems that are managed by ePolicy Orchestrator.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Navigate to **System Tree**, select a group or systems, then click the **Assigned Policies** tab.
3. Select a product from the product list, select a policy, then click **Edit Assignment**.
4. Select the policy to assign, select appropriate inheritance options, then click **Save**.

Create a self-protection policy

Self-protection allows ePolicy Orchestrator administrators to enable password protection for preferences in the client interface for managed Macs.

Enabling password protection prevents local users from modifying preferences that are defined by the ePolicy Orchestrator administrator, and prevents uninstalling the software on managed Macs. When local users try to modify preferences or try to uninstall the software, the application prompts for the ePolicy Orchestrator password.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. From the **Policy Catalog**, select **Endpoint Protection for Mac 2.1.0:General** as the product, then select **General Policies** as the category.
3. Click **New Policy**, type a name for the policy, then click **OK**.
4. On the **General** tab, define these options:
   - **Administrator password to unlock client preferences** — To enable or disable the password protection.
   - **Set password**
     - **Password** — Type the password.
     - **Confirm Password** — Confirm the password.

   The password must be at least 8 characters.
5. Click **Save**.
6. In the **System Tree**, select the systems or groups.
7. In the right pane, click the **Group Details** tab, then click **Wake Up Agents**.
8. In **Force policy update**, select **Force complete policy and task update**, then click **OK**.

   We recommend that you enable the password protection for preferences to prevent local users from modifying preferences that are defined by the ePolicy Orchestrator administrator, and to prevent local users from uninstalling the software on managed Macs.

Create an anti-malware policy

Create anti-malware policies to define parameters for an on-access scan and on-demand scan.

You can also create or modify these policies from the **System Tree**, while assigning policies to selected systems. See the product guide for your version of ePolicy Orchestrator for more information.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. From the **Policy Catalog**, select **Endpoint Protection for Mac 2.1.0: Anti-malware** as the product, then select **Anti-malware** as the category.
3. Click **New Policy**, type a name for the policy, then click **OK**.

4 On the **General** tab of the policy page, select these options:

- **General policies controlling overall functioning of Anti-malware** — To enable or disable the on-access scan and on-demand scan.
- **Anti-malware update** — To disable the local auto update schedule.

5 Click the **On-access Scan** tab and define these settings:

In...	Define...
On-access Scan policies	• **Scan contents of Archives and compressed files** — To scan archived and compressed files. • **Scan Apple Mail Messages** — To scan Apple mail messages. • **Scan file on Network Volumes** — To scan the files on the mounted network volumes. • In **Maximum scan time (seconds)**, type a value between 10 and 999.
Scan files	• **On Read** — To scan files when you access them to read. • **On Write** — To scan files when they are written to the hard disk. • **Read & Write** — To scan files when they are read from or written to the hard disk.
When a virus is found	• **Clean** — To clean the item that contains malware. • **Quarantine** — To isolate the item that contains malware. • **Delete** — To delete the item that contains malware. • **Notify** — To notify when malware is detected.
If the above action fails	• **Quarantine** — To isolate the item that contains malware. • **Delete** — To delete the item that contains malware. • **Notify** — To notify when a malware is detected.
When a spyware is found	• **Clean** — To clean the item that contains spyware. • **Quarantine** — To isolate the item that contains spyware. • **Delete** — To delete the item that contains spyware. • **Notify** — To notify when spyware is detected.
If the above action fails	• **Quarantine** — To isolate the item that contains spyware. • **Delete** — To delete the item that contains spyware. • **Notify** — To notify when spyware is detected.

6 Click the **On-demand Scan** tab, then define these settings:

In..	Define..
On-demand Scan policies	• **Scan contents of Archives and compressed files** — To scan archived and compressed files. • **Scan Apple Mail Messages** — To scan Apple mail messages. • **Scan file on Network Volumes** — To scan files on mounted network volumes.
When a virus is found	• **Clean** — To clean the item that contains malware. • **Quarantine** — To isolate the item that contains malware. • **Delete** — To delete the item that contains malware. • **Notify** — To notify when malware is detected.
If the above action fails	• **Quarantine** — To isolate the item that contains malware. • **Delete** — To delete the item that contains malware. • **Notify** — To notify when malware is detected.
When a spyware is found	• **Clean** — To clean the item that contains spyware. • **Quarantine** — To isolate the item that contains spyware. • **Delete** — To delete the item that contains spyware. • **Notify** — To notify when spyware is detected.
If the above action fails	• **Quarantine** — To isolate the item that contains malware. • **Delete** — To delete the item that contains malware. • **Notify** — To notify when malware is detected.

When you run an on-demand scan on managed Macs, events are logged in ePolicy Orchestrator when the scan is started and completed successfully. For more information on events, see KB article 79259.

7 Click the **Exclusions** tab.

a In the **Exclude specific disks, files and folders** text box, type the path you want to exclude from scanning.

For example, to exclude the file excludethis.docx, which is on the desktop, type `/Users/user/Desktop/excludethis.docx`.

b Select **On-access-Scan** or **On-demand Scan** as needed to exclude these items.

8 Click **Save**.

If you disable the **On-access Scan** and **Spyware Scan** protection from ePolicy Orchestrator, the security status of the managed Mac still appears that **Your Mac is Secured**.

Schedule an anti-malware update

Schedule an update to keep the anti-malware and DAT files up to date.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. On the **Assigned Client Tasks** tab, click **Actions**, then select **New Client Task Assignment**.
   a. For product, select **McAfee Agent**.
   b. For **Task Type**, select **Product Update**.
   c. Click **Create New Task** to open the **Client Task Catalog**.
   d. Type a name for the task, select **Mac Engine** and **DAT** in **Signatures and engines** from **Package types**, then click **Save**. The task is listed under **Task Name**.
   e. Select the task, then click **Next**.
4. On the **Schedule** page, define the schedule for the task.
   a. In the **System Tree**, select the systems or groups where you want to assign the task.
   b. Set these values, then click **Next**.
      - **Schedule status**
      - **Schedule type**
      - **Effective period**
      - **Start time**
      - **Task runs according to**
      - **Options**
5. On the **Summary** page, click **Save**.
6. In the right pane, select **Group Details**, then click **Wake Up Agents**.
7. In **Force policy update**, select **Force complete policy and task update**, then click **OK**.

Schedule an on-demand scan

Schedule an on-demand scan to scan the managed systems for threats.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**.
   a. For **Product**, select **Endpoint Protection for Mac 2.1: Anti-malware**.
   b. For **Task Type**, select **On-Demand Scan Task**.
   c. Click **Create New Task** to open the **Client Task Catalog** page.
   d. Type a name for the task, then click **Save**. The task is listed in **Task Name**.
4. Select the task, then click **Next**.

5 Define these parameters, then click **Next**.

- **Schedule status**
- **Schedule type**
- **Effective period**
- **Start time**
- **Task runs according to**
- **Options**

6 In the **Summary** page, click **Save**.

7 In the **System Tree**, select the systems or groups where you assigned the task.

8 In the right pane, click the **Group Details** tab, then click **Wake Up Agents**.

9 In **Force policy update**, select **Force complete policy and task update**, then click **OK**.

Create an application protection policy

Create policies to define rules to run applications without restrictions, with restrictions, or to block the execution.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Policy Catalog**, select **Endpoint Protection for Mac 2.1.0:Application Protection** as the product, then select **Application Protection** as the category.

3 Click **New Policy**, type a name for the policy, then click **OK**.

4 Double-click the policy.

5 On the **General** tab, select options from **General Application Protection policies**.

6 On the **Rules** tab, click **Add** to open the **Add Application Rule** page.

7 Type the application name with its path.

For example, to create a rule for the application Chess, type `/Applications/Chess.app` in the **Name** field.

8 From the **Status** drop-down list, select one of these options, then click **OK**.

- **Allow execution with full network access**
- **Allow execution without network access**
- **Allow execution with restricted network access**
- **Deny execution**

> If you select **Allow execution with restricted network access**, specify the protocols.

9 On the **Exclusions** tab, click **Add** to open the **Add Application Exclusion** page.

10 Type the application name with its path, then click **OK**.

For example, to exclude the application Calculator, type `/Applications/Calculator.app` in the **Name** field, then click **OK**.

11 Click **Save**.

> If you disable the **Application Protection** from ePolicy Orchestrator, the security status of the managed Mac still appears that **Your Mac is Secured**.

Desktop firewall policy

Define firewall policies and rules and enforce them on a managed Mac to control incoming and outgoing network traffic.

McAfee Endpoint Protection for Mac uses the common McAfee Host Intrusion Prevention extension. This table lists the policies that you can create under each product category.

> Because desktop firewall uses the common McAfee Host Intrusion Prevention extension, the features specific to McAfee Host Intrusion Prevention for Windows are marked as **Windows Only**.

Product	Category	Available policies
Host Intrusion Prevention 8.0: Firewall	**Firewall Options (Windows, Mac)**	Policies to: • Enable or disable the regular or adaptive firewall protection on the managed Mac. • Define stateful firewall settings. • Retain existing client rules when enforce firewall policy.
Host Intrusion Prevention 8.0: Firewall	**Firewall Rules (Windows, Mac)**	Policies to: • Create firewall rules. • Create rule groups. • Add rules from catalog. • Add group from catalog.
Host Intrusion Prevention 8.0: Firewall	**DNS Blocking (Windows, Mac)**	Policies to block access based on domain names.
Host Intrusion Prevention 8.0: General	**Trusted Networks (Windows, Mac)**	Set the trusted network options with a list of addresses and subnets marked as trusted.

Create a desktop firewall policy

Create a desktop firewall policy and assign it to managed systems.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Policy Catalog**, select **Host Intrusion Prevention 8.0: Firewall** as the product, then select **Firewall Options (Win, Mac)** as the category.

3 Click **New Policy**, type a name for the policy, then click **OK**.

4 Select the options, then click **Save**.

From...	Set these options...
Firewall status	**Enabled** — To enable desktop firewall protection on managed Mac. • **Regular protection** — To allow network traffic, only when the network packet adheres to the rule's conditions. • **Adaptive mode** — To create an allow rule, when the network packet does not match the existing rule.
Firewall client rules	**Retain existing client rules when this policy is enforced** — To retain the rules that are created by the client Mac when you enforce this policy.
Stateful firewall settings	**FTP protocol inspection** — Add a value for **TCP connection timeout (in seconds)** and **UDP and ICMP echo virtual connection timeout (in seconds)**.

5 Send an agent wake-up call.

> ℹ If the desktop firewall protection is disabled from ePolicy Orchestrator, the security status of the managed Mac still appears that **Your Mac is Secure**.

Create firewall rules

Define rules and parameters to allow or block a particular network's traffic.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Policy Catalog**, select **Host Intrusion Prevention 8.0: Firewall** as the product, then select **Firewall Rules (Windows, Mac)** as the category.

3 Click **New Policy**, type a name for the policy, then click **OK** to open the policy page.

4 Click **New Rule**, type a name for the policy, then click **OK** to open the **Firewall Rule Builder** page.

5 On the **Description** tab, define options, then click **Next**.

From...	Configure these options...
Name	Type a name for the rule.
Action	• **Allow** — To allow traffic. • **Block** — To block traffic. ℹ If you select **Block**, the **Treat match as intrusion** option is enabled. But this option is for **Windows Only**. Select **Log matching traffic**, if needed.
Direction	• **In** — To apply the rules for incoming traffic. • **Out** — To apply the rules for outgoing traffic. • **Either** — To apply the rules for incoming and outgoing traffic.
Status	• **Enabled** — To enable the rule on the managed Mac. • **Disabled** — To disable the rule on the managed Mac.

6 Define options on the **Network Options** page, then click **Next**.

From..	Configure these options..
Network protocol	1 Select • **Any Protocol** — To allow any IP Protocol. • **IP Protocol** — To select IPv4 Protocol. McAfee Endpoint Protection for Mac supports only IPv4 Protocols. IPv6 Protocol and Non-IP Protocol is for **Windows Only** 2 Select appropriate values for: • **New (Local)** • **New (Remote)** • **Add From Catalog (Local)** • **Add From Catalog (Remote)**
Media Types	Check • **Wired** — To apply the rule for wired connections. • **Wireless** — To apply the rule for wireless connections. • **Virtual** — To apply the rule for virtual connections. You can check more than one option in **Media types**.

7 Define options on the **Transport Options** page, then click **Save**.

From...	Configure these options...
Transport protocol	• **All Protocols** — To allow TCP, UDP, and ICMP protocols. • **TCP** — To allow only TCP protocol. • **UDP** — To allow only UDP protocol. • **ICMP** — To allow only ICMP protocol. **ICMPv6** option is for **Windows Only**.

8 Review the summary, then click **Save**.

> You don't need to define the **Applications** and **Schedule** tab settings because they apply to Windows configuration.

9 Send an agent wake-up call.

> For details on agent wake-up calls, see *Assign policies*.

Create a rule group and move rules to the group

Create a rule group and add rules to the group for easier management of rules.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Policy Catalog**, select **Host Intrusion Prevention 8.0: Firewall** as the product, then select **Firewall Rules (Windows, Mac)** as the category.

3. Click **New Policy**, type a name for the policy, then click **OK**.
4. On the **Firewall Rules page**, click **New Group**, type a name for the group, select **Direction** and **Status**, then click **Next**.
5. On the **Location** tab, define the options according to your requirements, then click **Next**.
6. On the **Network Options** tab, define the needed options, then click **Next**.
7. On the **Transport Options** tab, define the **Transport protocol**, click **Save**, then click the **Summary** tab.

   The **Application** and **Schedule** pages are used only for Windows configuration.

8. Verify the configuration details, then click **Save**. The rule group appears on the **Firewall Rules** page.
9. Select the rule group, then click ▶ to expand the rule group.
10. Select the rule that you want to move to the rule group, then click **Move Up** or **Move Down** according to the rule's position toward the rule group, until the rule is moved into the rule group.
    - Click **Move Up** if the rule appears after the rule group.
    - Click **Move Down** if the rule appears before the rule group.

    Always expand the rule group before moving rules into the group. Otherwise, the rules are not placed inside the rule group.

Create a DNS blocking policy

Create policies to block access to unwanted domains.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. From the **Policy Catalog**, select **Host Intrusion Prevention 8.0: Firewall** as the product, then select **DNS Blocking (Windows, Mac)** as the category.
3. Click **New Policy**, type a name for the policy, then click **OK** to open the policy page.
4. In **Blocked Domains**, type the domain name, click +, then click **Save**.

   You can add more domains in a single policy by clicking +.

Create a trusted networks policy

The trusted networks policy maintains a list of network addresses and subnets that you can tag as trusted. You can then apply the firewall rules to the tagged addresses.

You can include the local subnet address (with respect to the IP address of the managed Mac) as part of the trusted list. Additional subnets and single IP addresses can be added or removed from this list as needed.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. From the **Policy Catalog**, select **Host Intrusion Prevention 8.0: General** as the product, then select **Trusted Networks (Windows, Mac)** as the category.
3. Click **New Policy**, type a name for the policy, then click **OK** to open the policy page.
4. Enable **Include Local Subnet Automatically** to treat all users on the same subnet as trusted.
5. In **Trusted Networks**, type a trusted IP address, address range, or subnet.
6. Select **Trust for IPS** to define the network as trusted for network IPS signatures or HTTP type host and custom IPS signatures.

> Click + or − to add or remove a trusted network entry.

Create a location awareness policy

A location awareness policy allows user to access the network from multiple locations with a unique security policy for each location.

A location awareness policy contains a set of defined rules. When a network packet matches certain criteria with the group definitions, such as **ePO reachability** or **DNS server** address, the group becomes active. When the location awareness group is active, the network packet matches the rules in the group.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. From the **Policy Catalog**, select **Host Intrusion Prevention 8.0: Firewall** as the product, then select **Firewall Rules (Windows, Mac)** as the category.
3. Click **New Policy**, type a name for the policy, then click **OK** to open the policy page.
4. Click **New Group** to open the **Firewall Group Builder**.
5. Type a name for the **Group**, select **Direction** and **Status** options, then click **Next**.
6. On the **Location** tab, define these parameters, then click **Next**.
    - **Location status**
    - **Name**
    - **ePO reachability**
    - **Connection specific DNS suffix**
    - **Default gateway**
    - **DHCP server**
    - **DNS server**
    - **Primary WINS**
    - **Secondary WINS**
7. On the **Network Options** tab, define the parameters for **Network protocols** and **Media type**, then click **Next**.
8. On the **Summary** tab, verify the parameters, then click **Save**.

Queries and reports

Run predefined queries to generate reports, or modify them to generate custom reports.

Query	Displays
EPM: Anti-malware Compliance	The current Endpoint Protection for Mac: Anti-malware version compliance.
EPM: Anti-malware Threats	A line chart of the number of internal virus detections.
EPM: Anti-malware Version	Client versions for Endpoint Protection for Mac: Anti-malware.
EPM: Application Protection Version	Client versions for Endpoint Protection for Mac: Application Protection.
Host IPS: Client Versions	Top three client versions with a single category for all other versions.
Host IPS: Count of Firewall Client Rules	Number of firewall client rules created over time.
Host IPS: Count of Firewall Status	Where firewall is protection is enabled or disabled on managed systems.
Host IPS: Firewall Client Rules By Protocol / Port Range	Firewall client rules listed by protocol and port range.
Host IPS: Firewall Client Rules By Protocol / System Name.	Firewall client rules listed by protocol and system name.

Run a query

Run queries to generate reports based on data from McAfee Endpoint Protection for Mac.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as administrator.
2. Click **Menu** | **Reporting** | **Queries & Reports**.
3. From **Shared Groups** in the **Groups** pane, select the group.
4. Select a query from the **Queries** list, then click **Actions** | **Run**.
5. Click the item in the results list to view the details.

6 Troubleshooting

Identify and troubleshoot issues when using McAfee Endpoint Protection for Mac.

Run the repairMSC utility

Use the repairMSC utility to troubleshoot McAfee Endpoint Protection for Mac issues. It generates diagnostic reports, which can be uploaded to the McAfee server for analysis.

Task

1. Open a Terminal window, type the following command, then press **return**.

   ```
   /usr/local/McAfee/repairMSC
   ```

2. Type the administrator password when prompted, then press **return**.

3. Type `Y` to continue, then press **return**.

   A consolidated diagnostic report is generated in home directory for issue analysis. A list of issues appears with each category relating to a number from 1 to 8.

4. Type a number that best describes the issue, then press **return**. The repairMSC runs a repair utility based on the number selected and provides a solution.

5. Type `y` or `n` to confirm whether the issue was fixed, then follow the on-screen instructions.

   The report file repairMSC.zip is available in your home directory. `(Users/user)`.

   ℹ Contact McAfee Support for troubleshooting assistance.

Index

A

about this guide 7
adaptive mode 43
adaptive rules 45
anti-malware
  best practices 38
  configuring anti-malware 38
  defining exclusions 38
  testing the feature 24
  updating DAT files 31
anti-malware update, ePolicy Orchestrator
  scheduling 61
application protection
  configuring preferences 39
  creating rules 40
  defining exclusions 41
  modifying rules 41
  reapplying rules 41
  testing the feature 24

B

best practices
  configuring application protection 42
  firewall rules 53

C

check-in package, ePolicy Orchestrator
  checking in package 22
command-line installation 16
configuration
  general preferences 35
  proxy settings 54
  repository list 54
  scan task 32
  scheduling anti-malware engine update 55
conventions and icons used in this guide 7

D

dashboard
  view events summary 29
  view security status 29
default settings 19
  anti-malware 19
  general 19
  repository list 19
deployment, ePolicy Orchestrator 23
desktop firewall
  creating rules 49
  editing rule 49
  rules 47
  stateful filter 44
  testing the feature 25
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7
Domain Name System (DNS) 46

E

EICAR test file 24
events
  viewing details 30
  viewing summary 30
examples, firewall rules 51

F

features
  product 11
  protection, viewing status 29
firewall rules
  examples 51
  organization 48

H

how the software works 10

I

installation
  command line 16
  extensions 23
  on managed Macs 16
  on standalone Macs 16
  silent 16
  testing 24

installation *(continued)*
- using wizard 16

introduction 9

M

malware
- quarantine 31
- removing quarantined items 31
- restoring quarantined items 31

McAfee ServicePortal, accessing 8

N

need for security 9

O

on-access scan 36

on-demand scan 32
- configuring preferences 37
- creating a task 32
- removing scan task 33
- scheduling for standalone Mac 32
- scheduling from ePolicy Orchestrator 62

P

packages
- checking in 22
- details 16

policies
- assign 58
- available policies 64
- create 58
- management 57
- modify 58

policy creation
- anti-malware 59
- application protection 63
- desktop firewall 64
- DNS blocking 67
- location awareness 68
- trusted network 67

post installation tasks 20

preferences
- switching 35

Q

quarantine
- malware 31
- removing malware 31
- restoring malware 31

queries, ePolicy Orchestrator 69

R

regular firewall protection 44

removal of quarantined item 31

removal of software 27

removal of software extension 28

reports, ePolicy Orchestrator 69

rule group
- grouping rules 66

rules creation, ePolicy Orchestrator
- desktop firewall 65

S

scan task
- create 32
- modify 33

ServicePortal, finding product documentation 8

silent installation 16

software
- deployment 21
- repair 71

standalone Mac
- protection preferences 35

stateful filter 44

stateful FTP 46

system requirements 15

T

Technical Support, finding product information 8